Cyber Security Outlook: The Day after Tomorrow

S.C. Leung

Hong Kong Computer Emergency Response Team Coordination Centre
Hong Kong Productivity Council

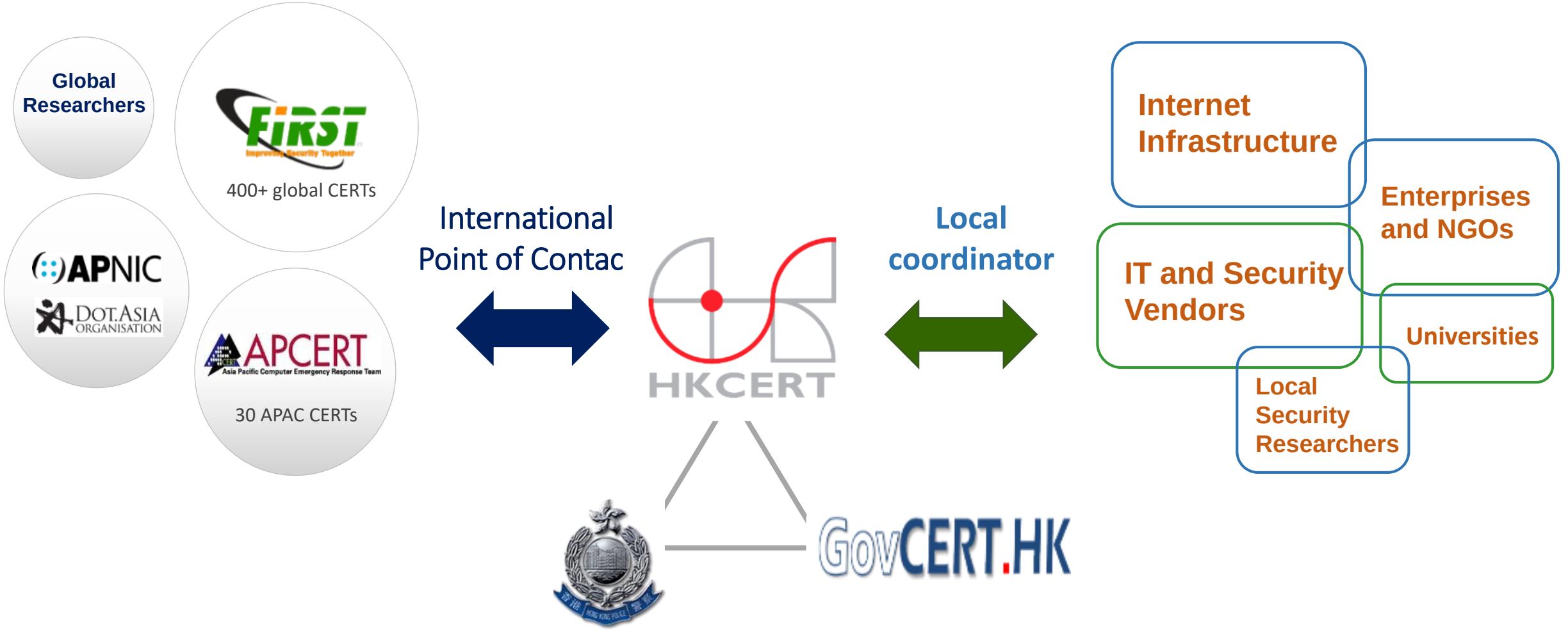
HKCERT

Hong Kong Computer Emergency Response Team Coordination Centre

- Established in 2001
- Funded by Government
- Operated by Hong Kong Productivity Council (HKPC)

We act as…

a point of contact on cross-border cyber security incidents



HKCERT Services

Free of charge service to Hong Kong Internet users and enterprises

- Incident Report

24-hr Hotline: 8105-6060

- Security Watch and Warning

Free subscription
https://www.hkcert.org/subscription

- Cross-border collaboration

- Awareness education and guideline

Cyber Security Landscape

- The Attackers
- The Vulnerabilities
- The Attacks
- Trend in 2018 and onwards

Attackers

Modern Attackers

Cyber Criminal

Hacktivist

Nation State

Image credits: Infographics of WatchGuard
http://www.bitrebels.com/technology/hacker-profiles-security-infographic/

Modern Attackers

Cyber Criminal

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

Image credits: Infographics of WatchGuard
http://www.bitrebels.com/technology/hacker-profiles-security-infographic/

Modern Attackers

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

Hacktivist

Image credits: Infographics of WatchGuard
http://www.bitrebels.com/technology/hacker-profiles-security-infographic/

Modern Attackers

Nation State

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

Image credits: Infographics of WatchGuard
http://www.bitrebels.com/technology/hacker-profiles-security-infographic/

What happened to SingHealth?

Impact of incident

Image source: TodayOnline

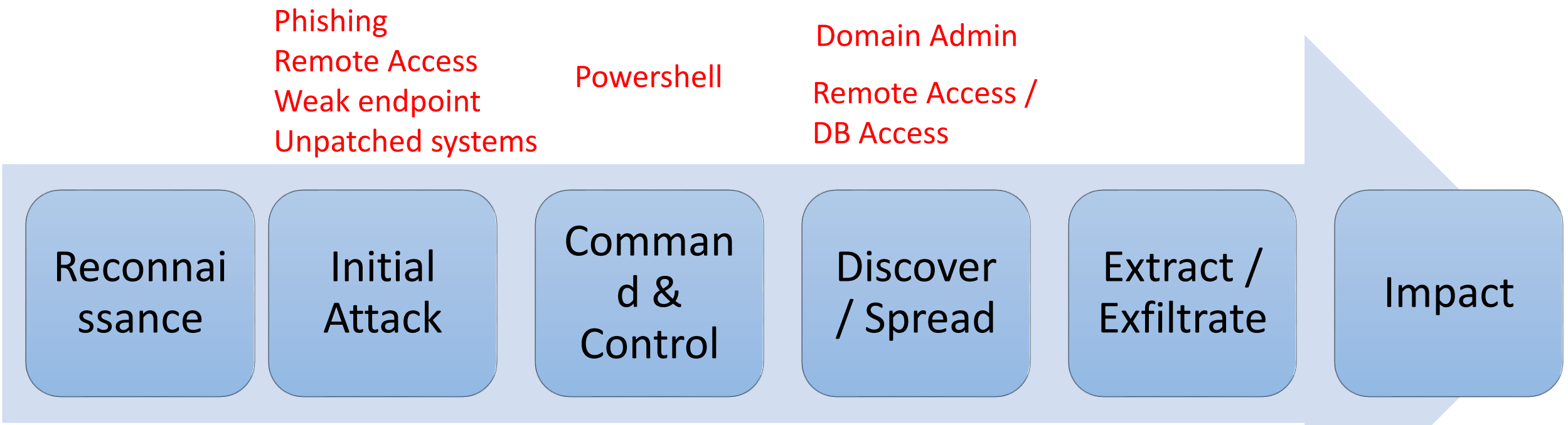
- 1.5 M non-medical patient data illegally accessed and copied (including Premier Lee)
- Attack started with a user workstation
- A Planned and organized attack – Advanced Persistent Threat
- Data was copied but not contaminated

SingCERT Advisory tells the story

- https://www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data

1. Review Domain Admin Accounts
2. Disable Powershell for Standard Workstations
3. Monitor Unauthorized Remote Access of Database Access
4. Tighten Control for Long-running or decommissioned Endpoints
5. Employ Strong Endpoint Protection
6. Keep System Up-to-date

Cyber Kill Chain



Collect info
Scan
Plan

Human /
System vuln.

- Phishing, malware
- Remote Access
- Unpatched System

- Take control of asset
- Set up comm. To attacker

- Expand the foothold
- Lateral movement
- Island hopping
- Until target reached

- Steal target data
- Export data (low and slow)
- Use alternate local export server

- Financial loss
- Damage of reputation

Source: Lockheed Martin's Computer Incident Response Team

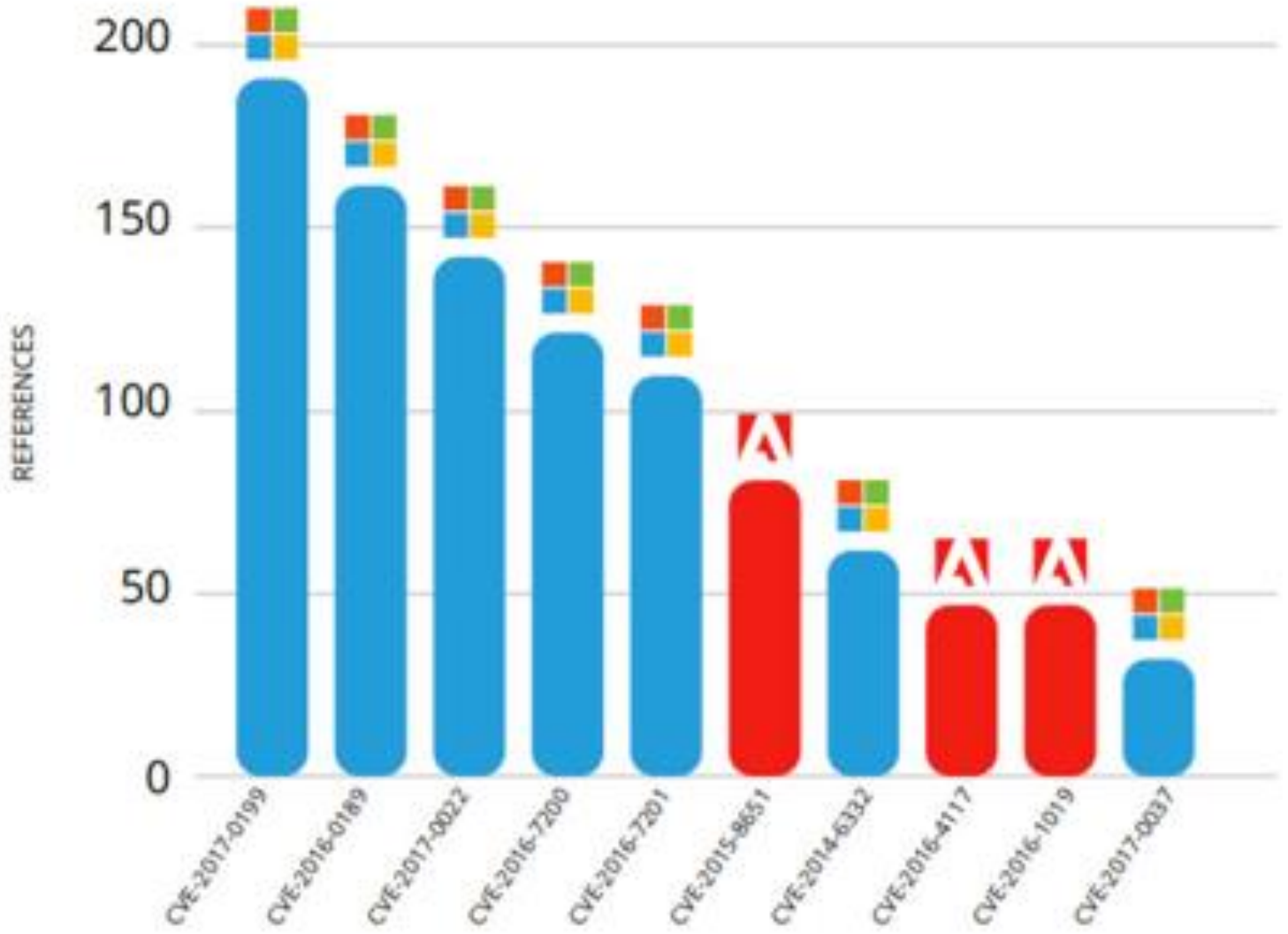
Lesson Learnt

- Cyber Attack Starts with anybody in the office
- It is not a matter to get in but STAY IN
- Lateral movement is key feature of Advanced Persistent Threat

Vulnerabilities

Top Vulnerabilities Targeted by Cyber Criminals in 2017

- Microsoft
  - Windows
  - Office
  - Internet Explorer
  - Edge
- Adobe
  - Flash Player



Source: Recorded Future

Shadow Broker leaked NSA Hacking Tools and Exploits

- 2017 April Shadow Broker released password for encrypted cache of NSA files.
  - Windows exploits
  - Protocols SMB, RDP, IMAP, HTTP
  - Tools for monitoring SWIFT interbank payments

Code Name		Solution
EternalBlue	SMB1, SMB2	Addressed by MS17-010
EmeraldThread	Print Spooler	Addressed by MS10-061
EternalChampion	SMB1	Addressed by CVE-2017-0146 & CVE-2017-0147
ErraticGopher	SMB1 WXP, WS2003	Addressed prior to the release of Windows Vista
EskimoRoll	Kerberos WS2000/2003/2008/2008R2	Addressed by MS14-068
EternalRomance	SMB1 WXP/W7/W8, WS2003/2003/2008/2008R2	Addressed by MS17-010
EducatedScholar	SMB2	Addressed by MS09-050
EternalSynergy	SMB1, SMB3 W8, WS2012	Addressed by MS17-010
EclipsedWing	Server RPC TCP/135	Addressed by MS08-067
EsteemAudit	**RDP** WXP, WS2003	Addressed by CVE-2017-0176 SA4025685
EnglishmanDentist	**Exchange Outlook WebAccess** WXP	Addressed by CVE-2017-8487 SA4025685
ExplodingCAN	**IIS6 with WebDAV** WS2003	Addressed by CVE-2017-7269 SA4025685

Some Statistics of Attacks

HKCERT

Incident Report Statistics

2017

HKPC

Cyber Security Readiness Index Survey

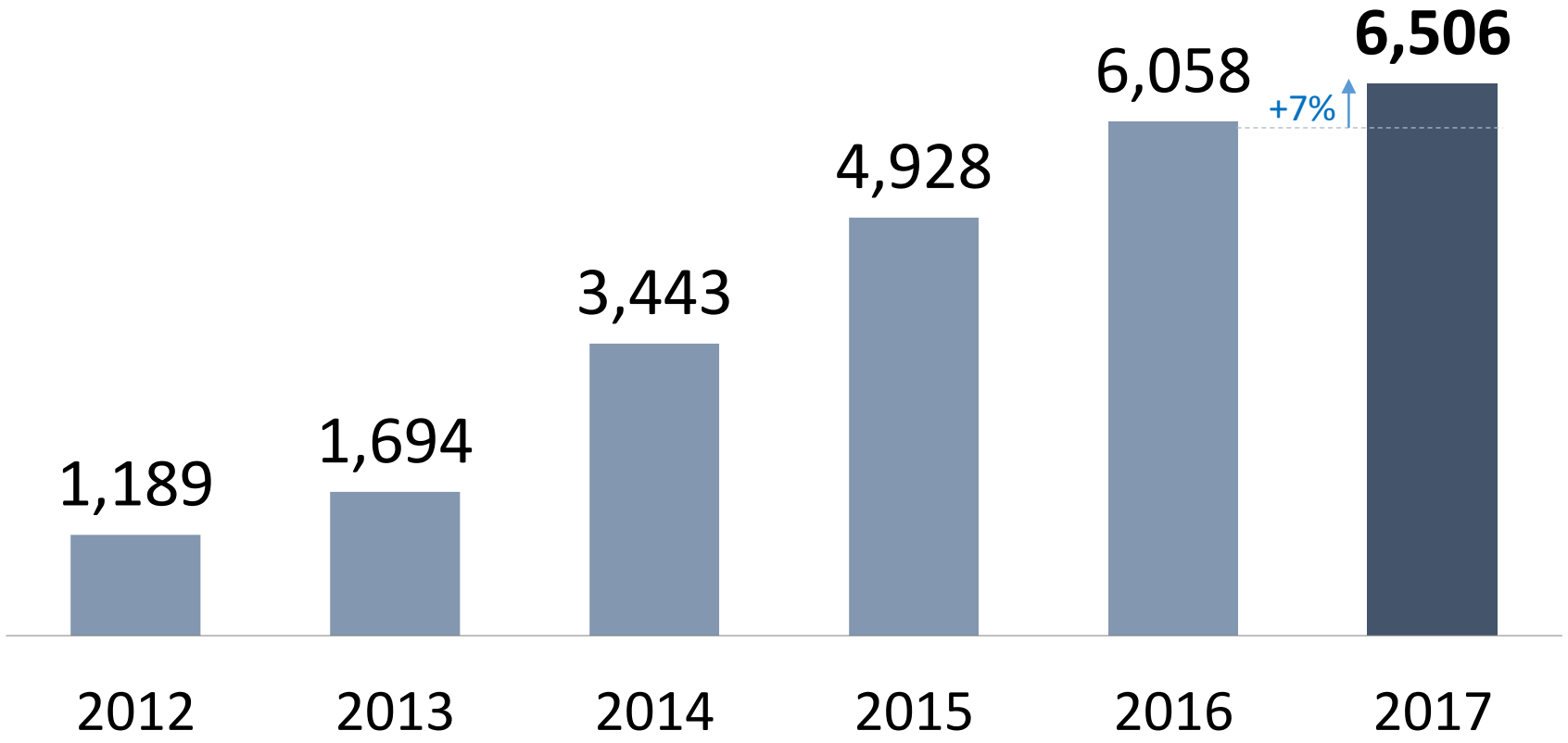
2018

HK Police

Cyber Fraud Statistics

2018 H1

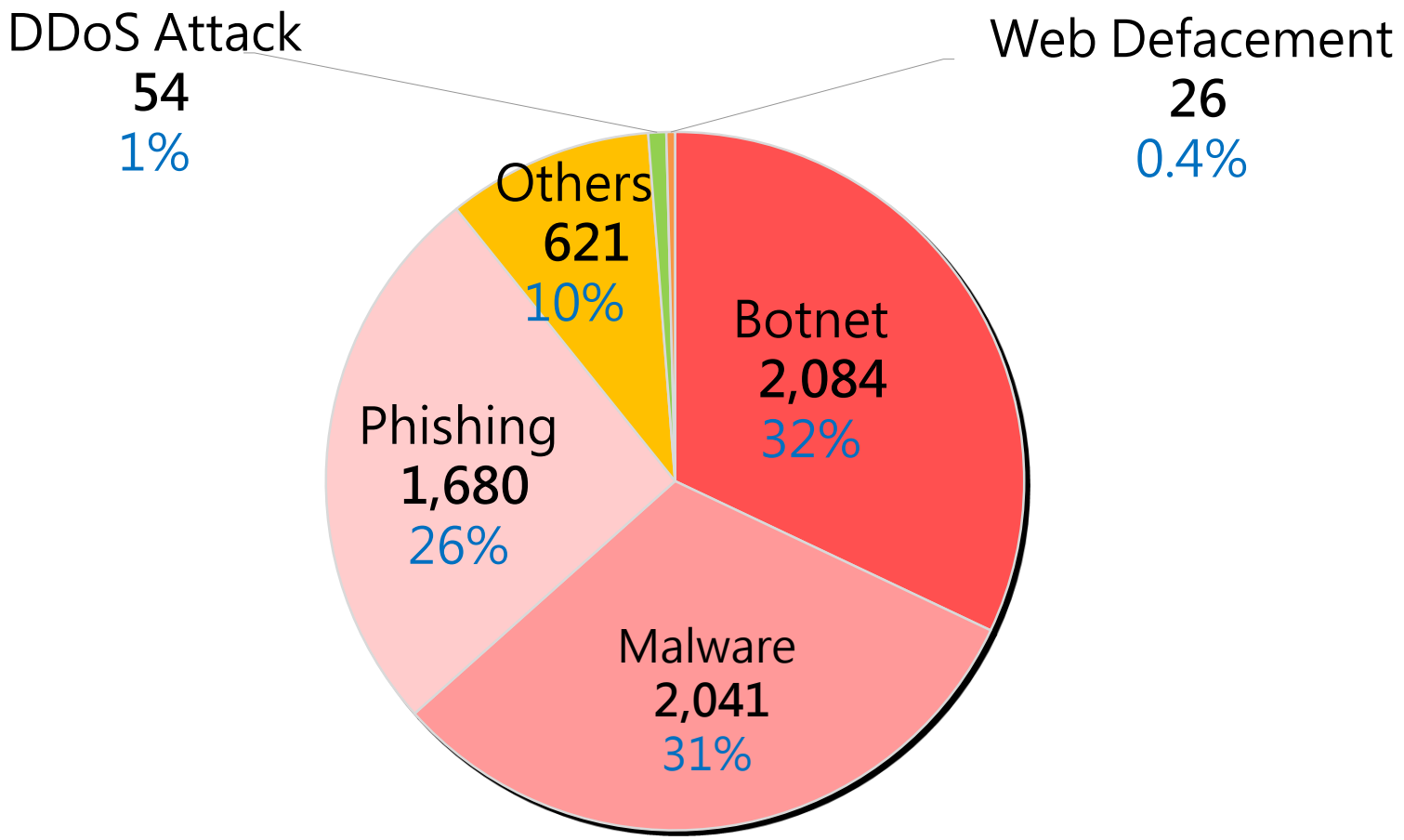
HKCERT Security Incident Reports



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

Source: HKCERT

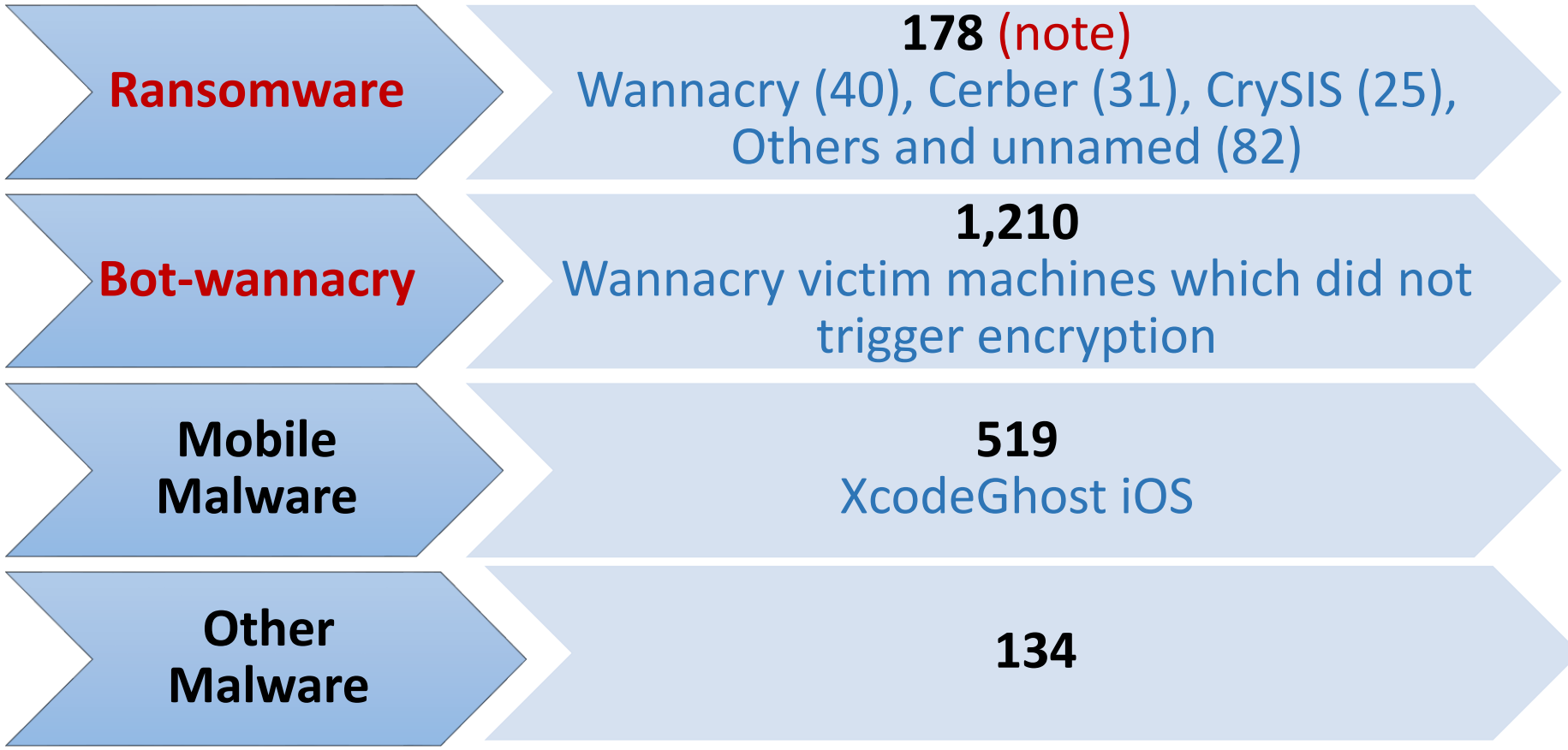
HKCERT Security Incident Reports



Source: HKCERT

Breakdown of Malware Incident Reports

- **Malware Incident Reports: 2,041**



Note: 309 ransomware reports (year 2016)

Source: HKCERT

Cyber Security Incidents in Past 12 Months

Ransomware	Phishing Email	CEO Scam	Other Malware including Botnet	DDoS
52%	49%	35%	25%	10%

SSH Hong Kong Enterprise Cyber Security Readiness Index Survey (2018 Mar)

Sample Size: SMEs: 300 Large Enterprises : 50

Source: HKPC

Police statistics on fraud crimes in 2018 H1

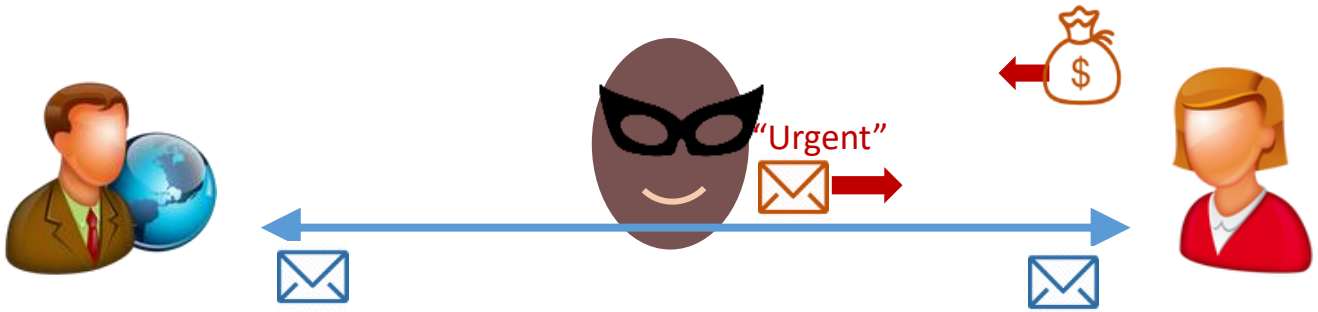
	2017 H1		2018 H1	
	# of Reports	Financial Loss (HKD)	# of Reports	Financial Loss (HKD)
CEO Email Scam	311	441M	402	759M
Investment Fraud	53	19.6M	90	536M
Internet romance fraud	78	36.4M	272	137M
Job search fraud	16	0.33M	69	11.4M
Phone Scam	443	147M	165	10.6M

Source: HK Police

Advanced CEO Email Scam (with malware)

- **Step 1: Sniff and Learn** (via malware or hacked email account)

- **Step 2: Launch attack** when CEO is on business trip



Trend in 2018 and onwards

HKCERT Outlook (Jan 2018)

1. **Financially Motivated Cyber Crimes** continue to proliferate
2. **Supply Chain Attacks** bypass Enterprise Defense
3. **More Regulation** for Security and Privacy
4. **Internet of Things (IoT) attacks** on the Rise
5. **Mobile Payment Apps** as New Attack Targets

Source: HKCERT

Crime-as-a-Service proliferating

- **One-stop attack service** (attack tools, infrastructure and Bitcoins payment service) **lowers entry barrier for layman criminals**

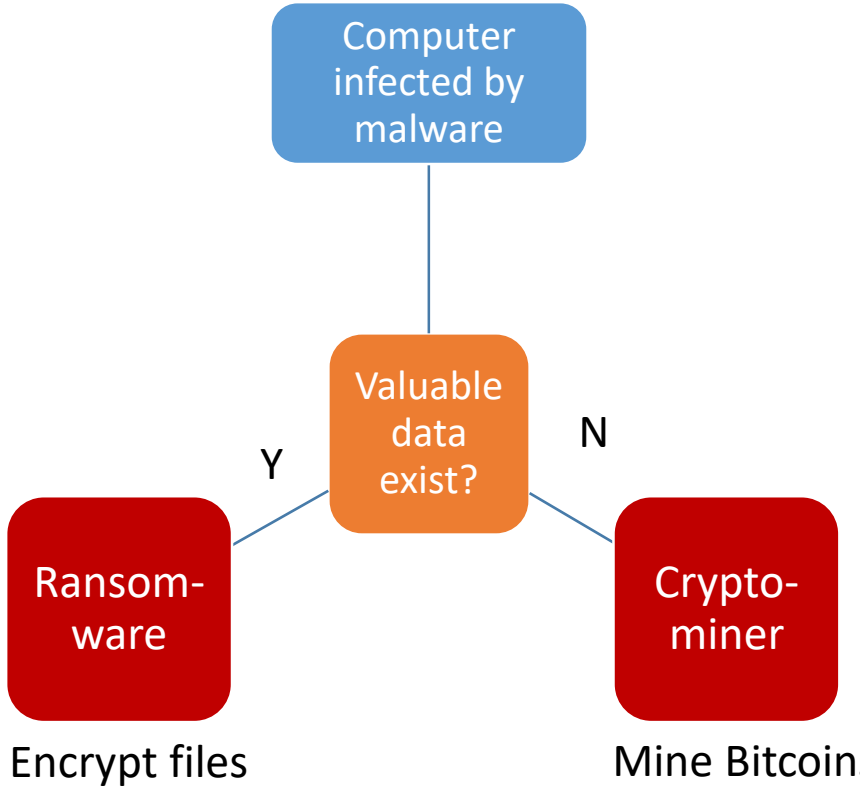
- Impact to the Industry
  - Extortion and fraud incidents likely continue to grow

Image credit: http://www.nicheapex.com

Recent Development of Ransomware

- Popular ransomware in 2018
  - CrySiS (via remote desktop service)
  - Cerber (via email attachment)

- Hybrid Malware
  - Ransomware + Coin-miner



https://www.hkcert.org/ransomware.hk/ransomware-kb.html

Recent Hacking Extortion in Travel Agencies

WWPKG 縱橫遊 (Nov 2017)

- Affected 200,000 Hong Kong users
- Attacker demanded millions of HKD in Bitcoins

BigLine 大航假期 (Jan 2018)

Goldjoy 金怡假期 (Jan 2018)

- Attacker claimed to compromise system obtaining customer data and demanded ransom

The listed cases are NOT necessarily reports received by HKCERT.

Digital Pump and Dump

the newpaper

BUSINESS

2016

Penny stock pump-and-dump fraud growing concern for HK

- Attacker control penny stock price via hijacked share trading accounts

Indian online broker Sharekhan targeted

(2018-Apr)

- Owned by BNP Paribas
- **Discovered attempts of unauthorised access**
- **Users advised to reset passwords and use 2FA**

https://www.sharekhan.com/articleDetails/10-tips-to-trade-safely-online

FBI warns of “unlimited” ATM Cashout scheme (2018-Aug)

- Fake ATM cards used to draw money in ATMs over 28 countries
- System compromised to remove the withdrawal limit

- An India bank lost US$13M
- A transaction of US1.93M was moved to a bank account in HK

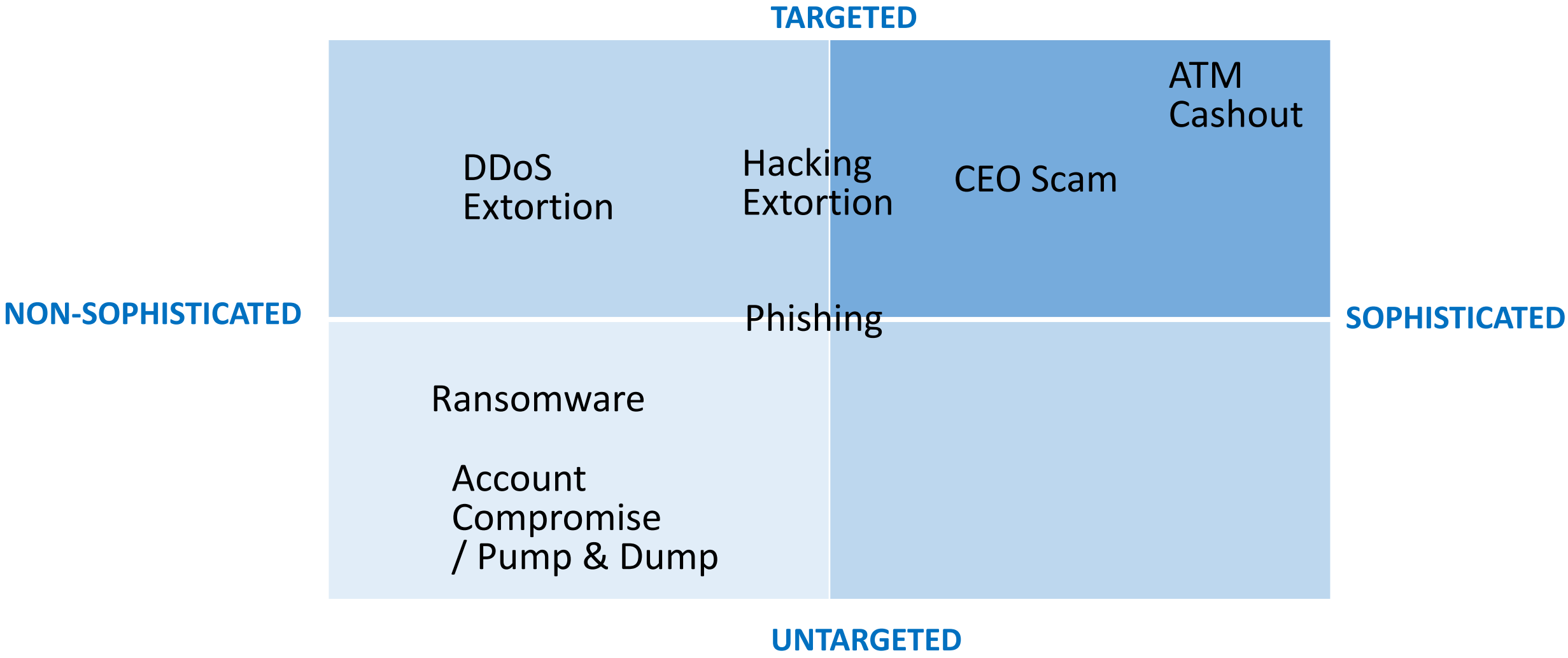
India's Cosmos bank raided for $13m by hackers

Report points finger at North Korea for cyber-heist

By Shaun Nichols in San Francisco 15 Aug 2018 at 20:05 10 SHARE

Image source: TheRegister

Financially Motivated Cyber Crimes continue to proliferate



Supply Chain Attacks bypass Enterprise Defense

- **Software Update mechanism** for attacking enterprise

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

- **Exploit visitors to compromised legitimate website**

Supply Chain Attacks bypass Enterprise Defense

Supply Chain Attacks in 2107

Software Update Contamination

- 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

Supply Chain Attacks bypass Enterprise Defense

Supply Chain Attacks in 2107

Browser Extension Contamination

- Eight Chrome extensions compromised Aug 2017
  - Attackers took over extension developers' Google account via phishing; then manipulate internet traffic and web-based ads

Legitimate Website Compromise

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

Next Wave of Ransomware

Spread mechanism		Force to demand ransom	
 Email scam with social engineering	Locky	 Pay ransom on time or your **DATA** is **DESTROYED**	Jigsaw
 Network worm	Wannacry	 Pay ransom on time or your **DATA** is **PUBLICIZED**	Doxware
 Time bomb. Targeted 	SamSam	 Pay ransom or **INFECT 2 friends** to get **DATA** back	Popcorn Time

Attacks on Internet of Things (IoT)

- **VPNFilter attack on IoT**
  - Infected 500K home or small office routers and NAS over 50 countries
  - A modular malware with wide range of capabilities
    - Intercept data and monitor network over Modbus protocol
    - Change webpage and insert artificial data to deceive user
    - Exfiltrate data using Tor
    - Launch DDoS
    - Destroy infected device with “kill” command
  - State-sponsored or state-affiliated threat actor might be behind the attack

AI & Cyber Security

AI and cyber security – Defenders' perspective

- Application of AI to prevent, detect cyber threats
- IRS consider to use AI in public and private sector cyber security
  - https://govmatters.tv/application-of-ai-to-prevent-detect-cyber-threats/

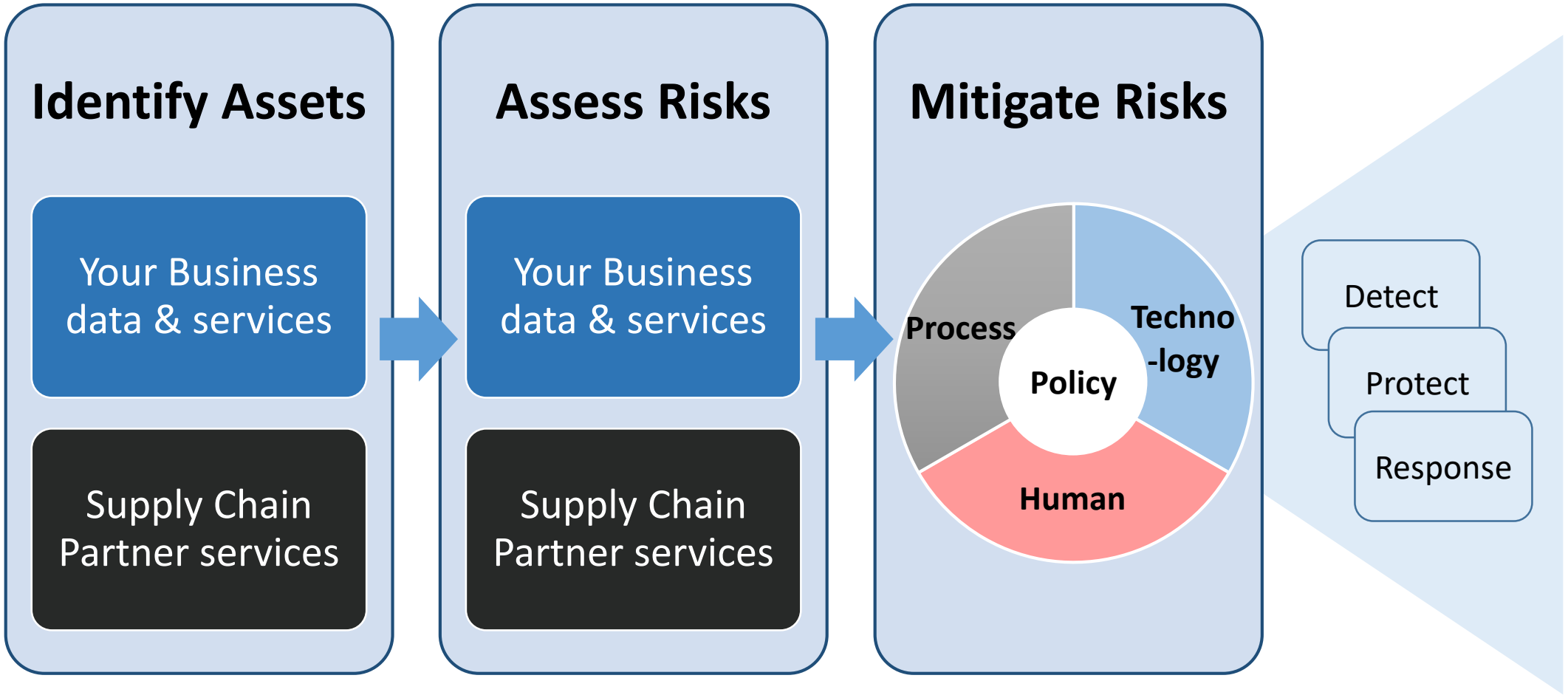
- Detecting malicious email via AI and machine learning
  - https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/outsmarting-email-hackers-using-ai-and-machine-learning

AI and cyber security – Attackers' perspective

- Ransomware PyLocker has anti-machine-learning feature.
  - Anti-sandbox: sleep for 11.5 days if infected system has <4GB memory, which means the environment might not be a real user PC
  - https://www.securityweek.com/new-python-based-ransomware-poses-locky

- IBM Research Lab developed a DeepLocker, a proof-of-concept AI assisted malware
  - The malicious content of the malware is locked until it meets a triggering condition – for example, the face of user matches the target. In normal days it is difficult to identity the malware.
  - https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

Build your Security Readiness



Build your Security Readiness

- **Process Controls**
  - **Minimize exposure** of data to the Internet and service providers / partners
  - **Apply Access Control: minimal privilege**
  - **Test software updates** before deployment
  - Tighten **fund transfer control** to tackle scams

Build your Security Readiness

➢Technology **Controls**

- **Close Loopholes**: patching, configuration, disable insecure services
- **Control incoming traffic**: remote access and privilege access
- **Block traffic** to malicious websites
- **Apply Security Best Practices in Mobile App development**
  - Remember to validating digital certificates (see reference for details)
- **Backup** data and keep an **offline copy**

Build your Security Readiness

➢ **Build Human Firewall**

- Organize Cyber Security Awareness Training and Drills
- Use alternative communication channel (e.g. phone) to verify transaction requests
- Advise to use strong passwords and **two-factor authentication**
- Stay vigilant to unsolicited email, website and when connecting to public wi-fi network

Build your Security Readiness

➢ Share and Collaborate

- Build trusted network to share cyber security information of common interest
- Provide global and local situational awareness; provide actionable data (e.g. bad IP address) to secure systems
- Collaborate in risk mitigation

Know Our Enemy **Better and Earlier** is

the Key to Defend Better

Cybersec Infohub

www.cybersechub.org

Programme Objectives

Programme of the Office of Government Chief Information Officer

Establish a cross-sector, trusted collaborative network to share cyber security information

Provide a collaborative platform for sharing information, to give a better visibility of cyber security situational awareness

Cultivate local collaborative culture among the industry for effective cyber security information sharing

To enhance the cyber resilience of Hong Kong against territory-wide cyber attacks

Cybersec Infohub

Cyber security İnformation to be shared

- Threat information and analysis
- Alerts, news, vulnerabilities
- Mitigation advisories

- Situational awareness
- Best practices and tips
- Strategic analysis

Key participants

ISPs

Critical Infrastructure

Critical Internet Infrastructure

IT & Security Vendors

Researcher

Local CERTs

Methods of Exchange

- Via the Platform
- Industry Event
- Tele-conference
- Webinar
- Working Group

The End

HKCERT

Web: www.hkcert.org

Email: hkcert@hkcert.org