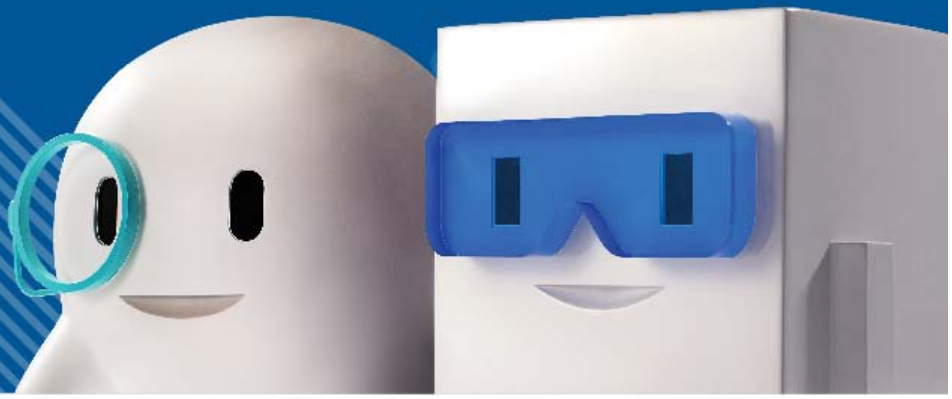
Koala Wong
資訊保安顧問
香港電腦保安事故調協中心

2018 Security Threat Landscape in Edu Sector



All-round Productivity Partner
全方位企業伙伴

2018-05-10

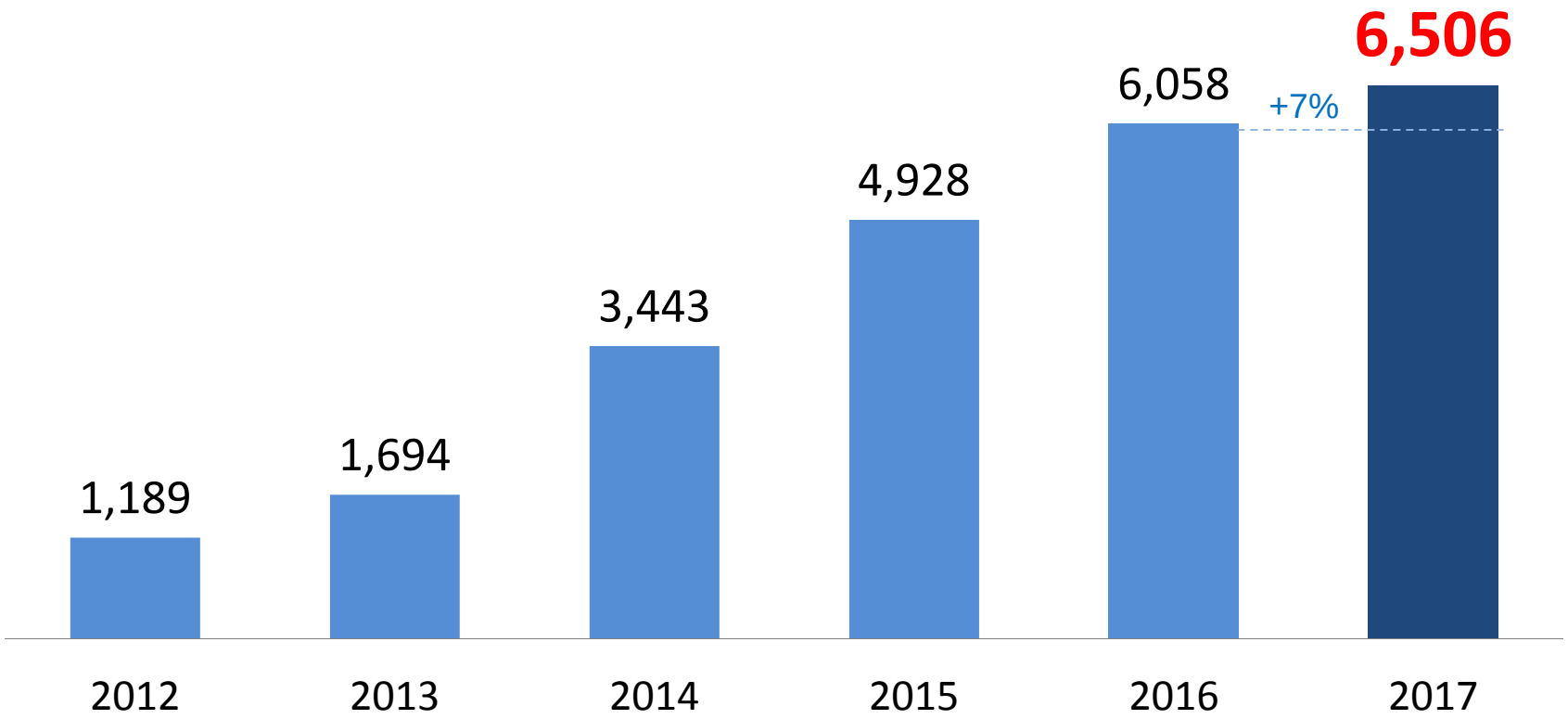
HKCERT 的服務

- 成立於 2001 年， 100% 政府資助，由**香港生產力促進局** (HKPC) 管理
- 服務範圍
  - 電腦保安警報監測及預警
  - 保安事故報告及求助
  - 出版資訊保安指引和資訊
  - 提高資訊保安意識
- 維持一個良好電腦保安協調網絡，包括本地及海外的機構，確保能有效地作出回應和處理

內容

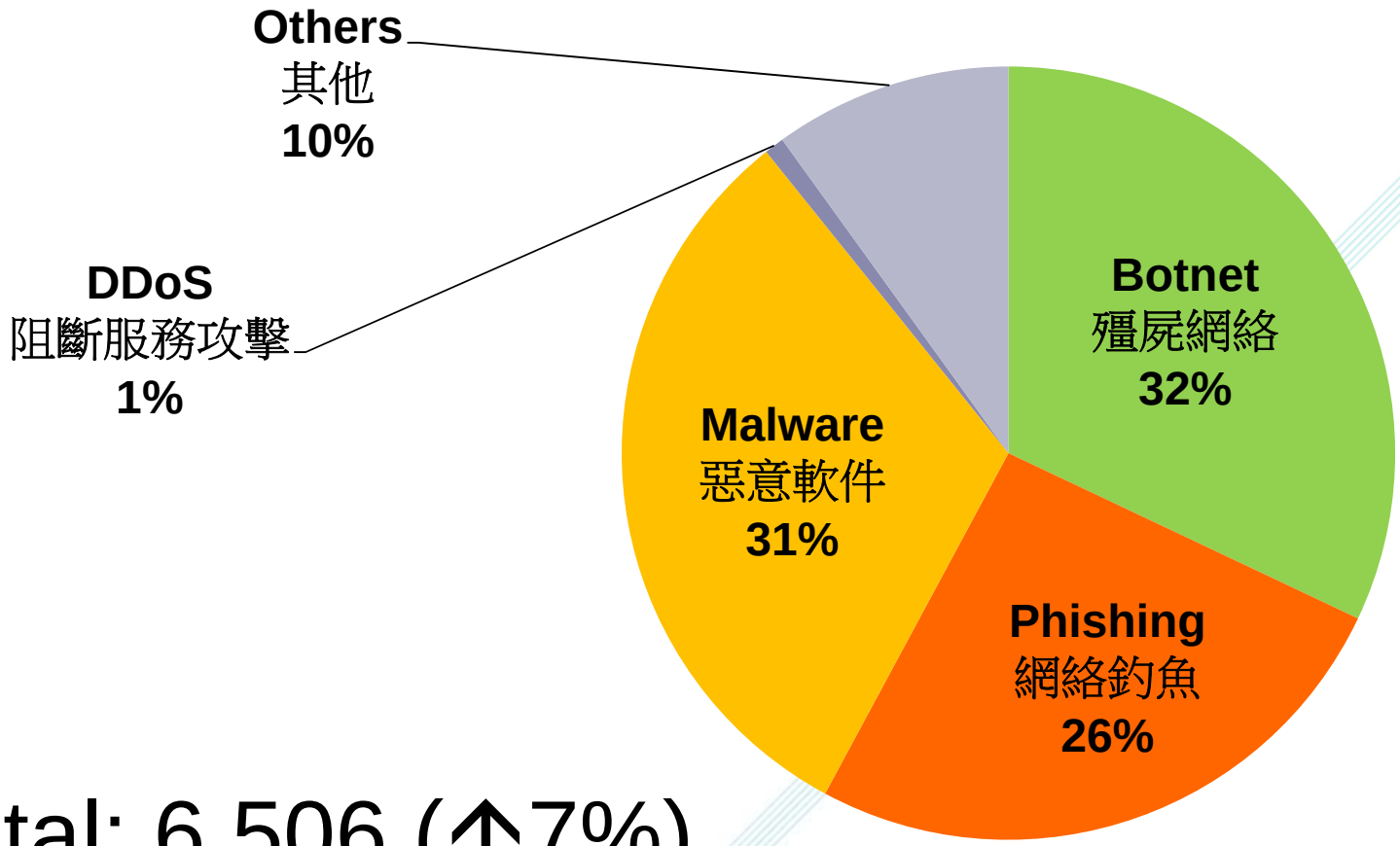
- 2017香港網絡保安威脅狀況
- 2018年保安展望
- 個案分享
- 網絡安全的保安心法

2017年電腦保安事故



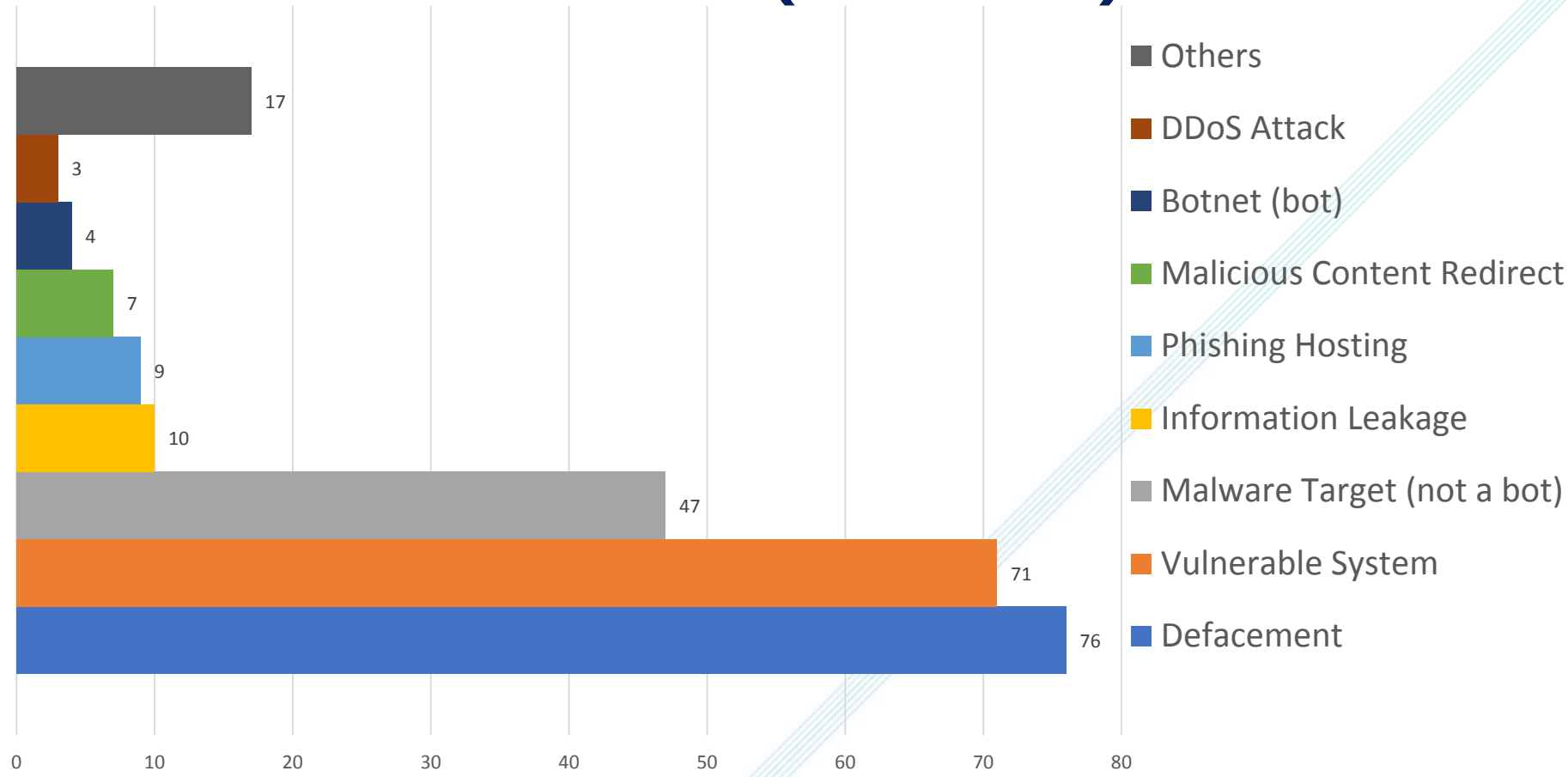
與全球資訊保安機構合作, 2017年 **91%** 個案屬於轉介個案。

2017 電腦保安事故報告的分佈



Total: 6,506 (↑7%)

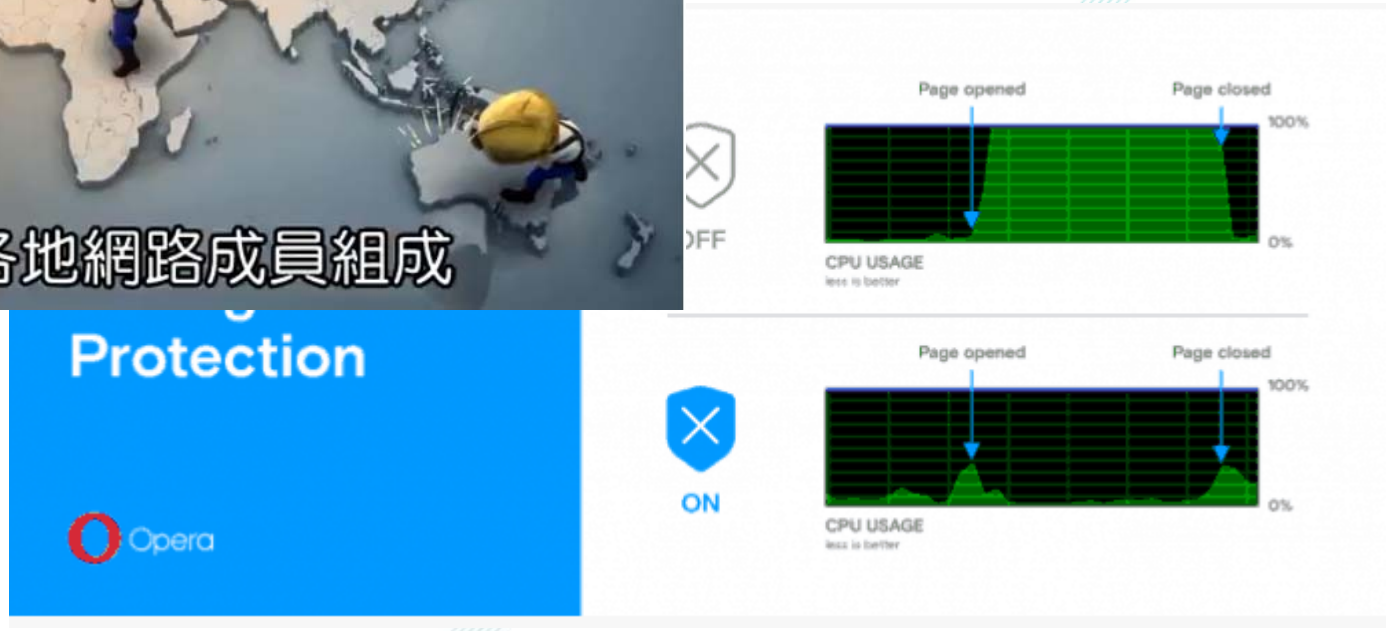
2016-2018電腦保安事故報告的分佈 (教育界)



案例：偷、呃、拐、騙

偷:惡意程式


懂財經 3D
世界各地網路成員組成


Protection
Opera
OFF
Page opened
Page closed
100%
0%
CPU USAGE
less is better
ON
Page opened
Page closed
100%
0%
CPU USAGE
less is better

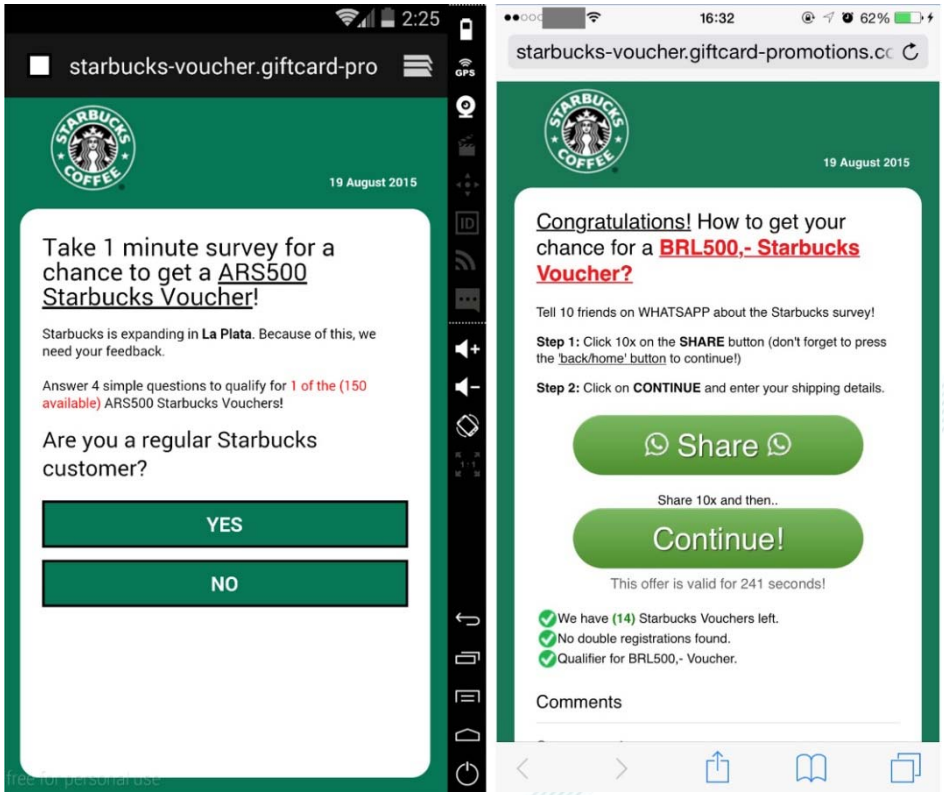
惡意程式的教訓

影響: 資料外洩 ($$$?), 電腦變慢

事件中的學習:

- 為電腦安裝保安軟件，包括防毒軟件、防火牆、網頁瀏覽的保護功能等
- 不要開啟來歷不明網址、連結
- 保持系統/應用程式更新

呃: 虛假優惠



https://securelist.com/blog/incidents/71942/youre-paying-for-your-starbucks-one-way-or-the-other/

呃: 虛假二維碼

虛假的教訓

影響: $$$$$

事件中的學習:

不要開啟來歷不明電郵/即時通訊訊息

- 使用新版本的瀏覽器，已加入惡意網站過濾功能
- 若有懷疑，請向相關機構核實內容
- 千萬不要未睇先 “Share”

拐: 勒索軟件


300,000 victims in 150 countries
Wanna Crypt v2.5
Ooops, your files have been encrypted!
English
not so enough time.
You can decrypt some of your files for free. Try now by clicking
But if you want to decrypt all your files, your need to pay.
3rd, some words like 'View' mean different things in different
that these keys should be some how chaged so we would be able
How Do I Pay?
different translations. I have some problems with specially this
which was used in different places, and there is one important
4th, in some places where place holders are used, the result will
not so enough time.
You can decrypt some of your files for free. Try now by clicking
But if you want to decrypt all your files, your need to pay.
characters, ...) in appropriate places to create better result in fina
Payment will be raised on
00:00:00
Your files will be lost on
00:00:00
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin this address:
115p7UMMngoj1pMvkpHijcRdfJNX
Copy
About bitcoin
Check Payment
Decrypt

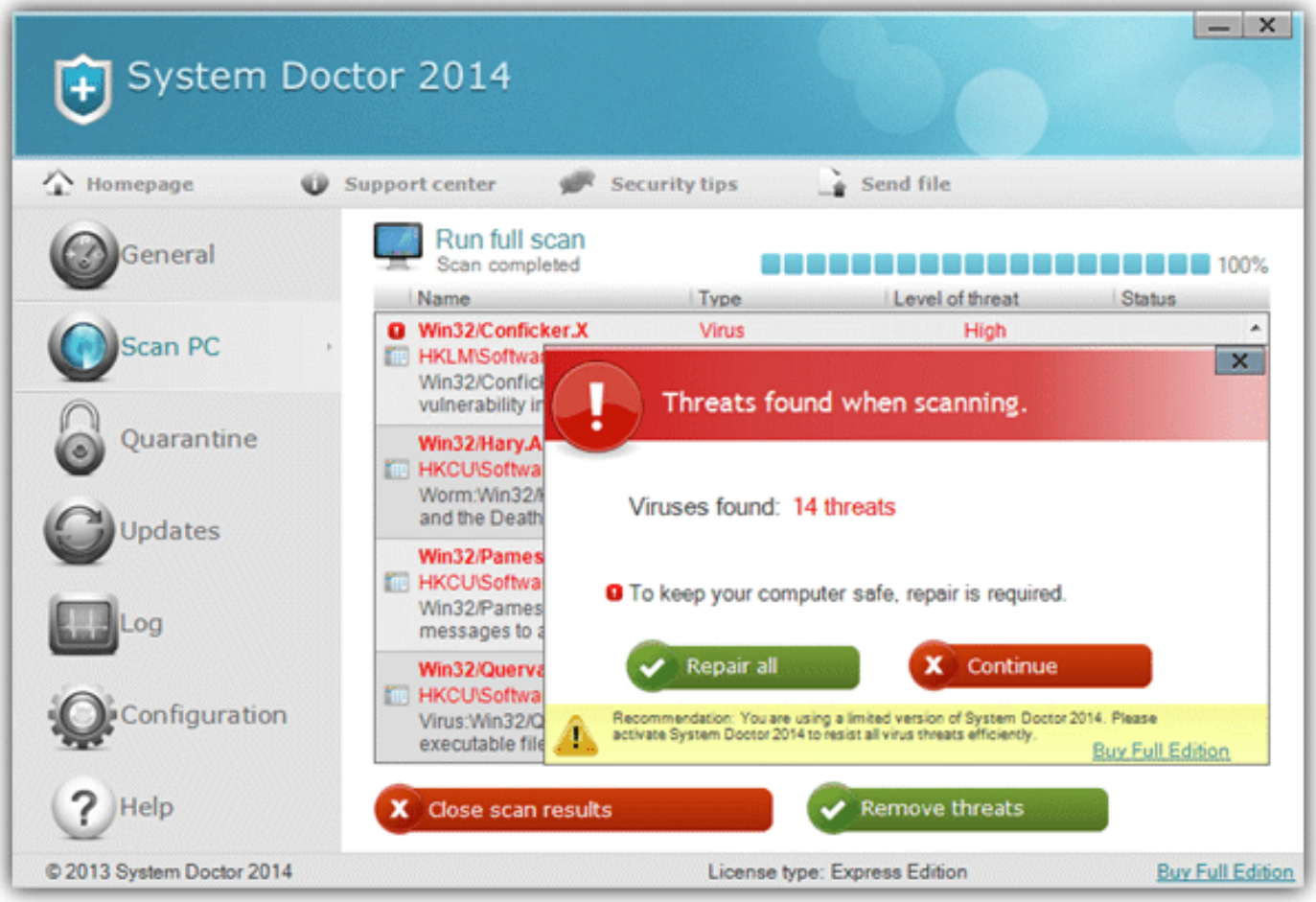
勒索軟件的教訓

影響: $$$$$

事件中的學習:

- 定期為檔案進行備份，並分開存放
- 若使用雲端備份，應啟用「版本紀錄」功能
  - PC 電腦 / Android 系統
    - 不要執行/安裝不明來歷程式
    - 為電腦安裝保安軟件

騙:偽裝(防毒)軟件


System Doctor 2014
Homepage
Support center
Security tips
Send file
General
Scan PC
Quarantine
Updates
Log
Configuration
Help
Run full scan
Scan completed
100%
Name
Type
Level of threat
Status
Win32/Conficker.X
Virus
High
Threats found when scanning.
Viruses found: 14 threats
To keep your computer safe, repair is required.
Repair all
Continue
Recommendation: You are using a limited version of System Doctor 2014. Please activate System Doctor 2014 to resist all virus threats efficiently.
Buy Full Edition
Close scan results
Remove threats
© 2013 System Doctor 2014
License type: Express Edition
Buy Full Edition

騙:偽裝軟件

供應鏈攻擊 繞過企業的防禦

偽裝軟件的教訓

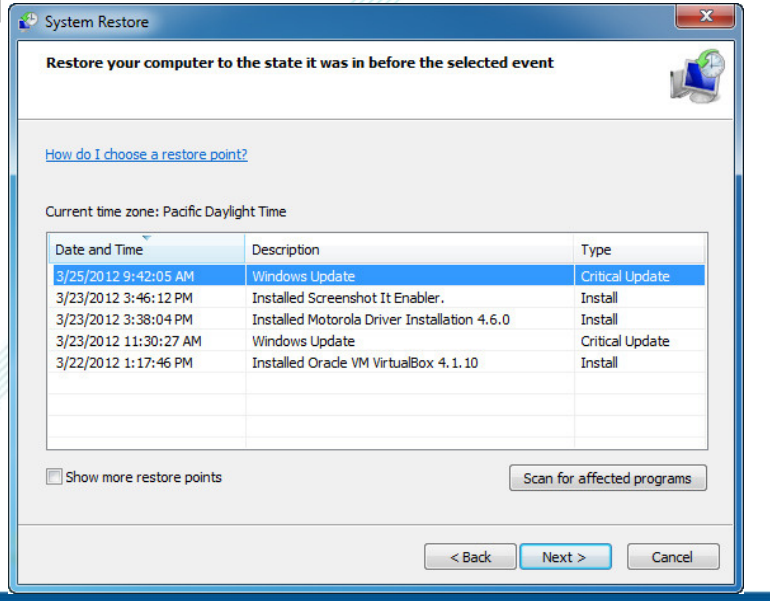
影響: 資料外洩 ($$$?)

事件中的學習:

- 為電腦安裝(真的)保安軟件

http://www.av-test.org/
http://www.av-comparatives.org/

- 啟動系統還原功能



2018年保安展望

1. **以金錢動機的網絡犯罪繼續蔓延**
2. **物聯網攻擊上升**
3. 流動付款程式或成為攻擊對象
4. 更多有關網絡安全和隱私的規管
5. **供應鏈攻擊繞過企業的防禦**

教育界

網絡保安的應對

- 程序控制 (Process Controls)

  - **資料儲存的保安**
  - **禁止/減少連接互聯網**
  - 加強訪問控制：最小權限
  - 在部署軟件更新之前測試軟件
  - 加強資金轉移程序以避免詐騙

網絡保安的應對

- 技術控制 (Technology Controls)
  - **堵塞系統的漏洞 :** 安裝修補程式、強化設定安全、停用不安全服務
  - **控制外界對內的訪問:** 遙距存取服務及特權存取
  - **堵截對外的惡意網站的訪問**
  - **備份數據，保持離線副本**

網絡保安的應對

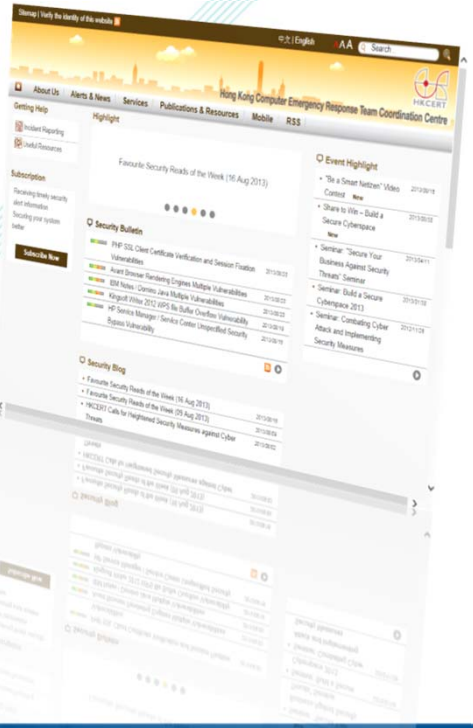
- 提高意識, 堵塞人為漏洞 (Human Firewall)

  - 舉辦**安全意識教育**及安全演習
  - 使用其他通訊渠道（例如電話）**驗證交易要求**
  - 使用較強的密碼及**雙重認證**
  - **格外小心**: 提防來歷不明的電子郵件和網站和公共 Wi-Fi 網絡

HKPC

香港電腦保安事故協調中心

- 訂閱資訊保安警報
  - https://www.hkcert.org/subscription
- 保安公告
  - https://www.hkcert.org/security-bulletin
- 保安工具
  - https://www.hkcert.org/security-tools



網址: https://www.hkcert.org

電郵: hkcert@hkcert.org