網絡安全對數據保護的重要性

LAWRENCE LAW
資訊保安顧問
香港電腦保安事故協調中心
20 SEP 2019

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)
香港電腦保安事故協調中心

Mission:

As the **Centre for coordination** of computer security incident response for local enterprises and Internet Users, and the **International Point-of-Contact**

- Founded in 2001
- Funded by Government
- Operated by Hong Kong Productivity Council

HKCERT services

HKCERT Website
www.hkcert.org

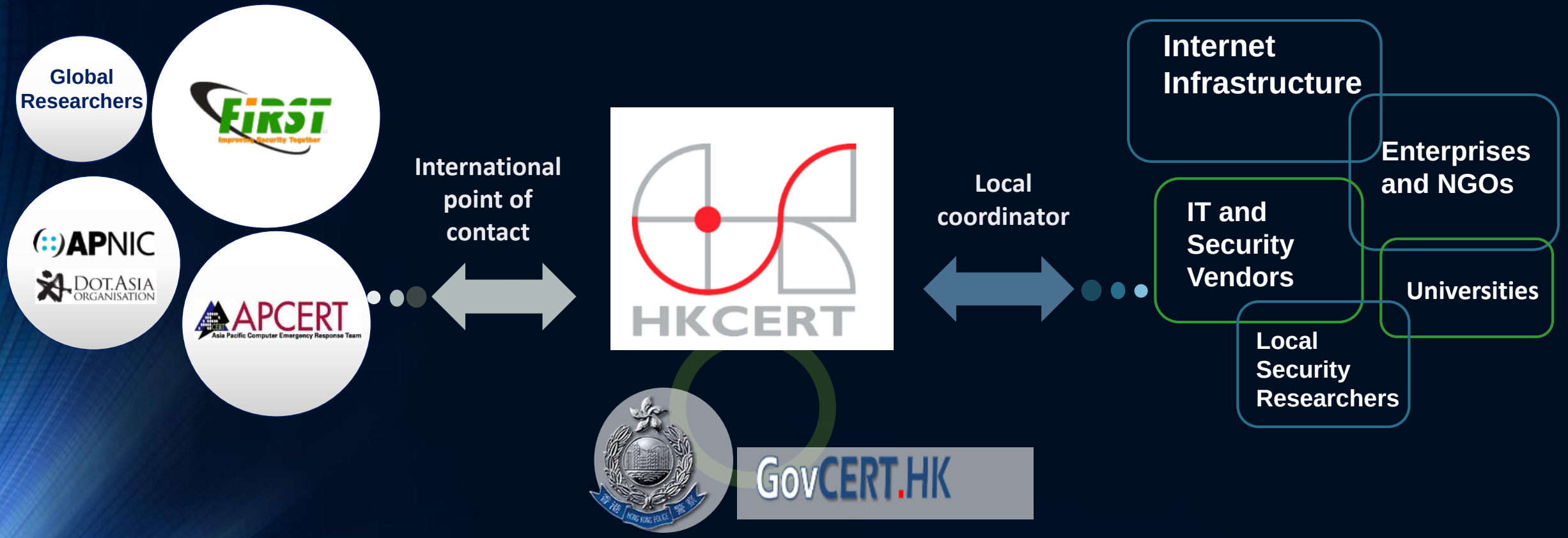
01 Monitoring and Early Warning
Free subscription

02 Incident Response
24-hr Hotline: 8105-6060

03 Publication of Security Guidelines and Information

04 Promotion of Information Security Awareness

HKCERT act as… Focal Point of cross-border cyber security incidents



議程

1. 網絡安全概況
2. 網絡安全的重要性
3. 認識網絡攻擊手法

網絡安全概況

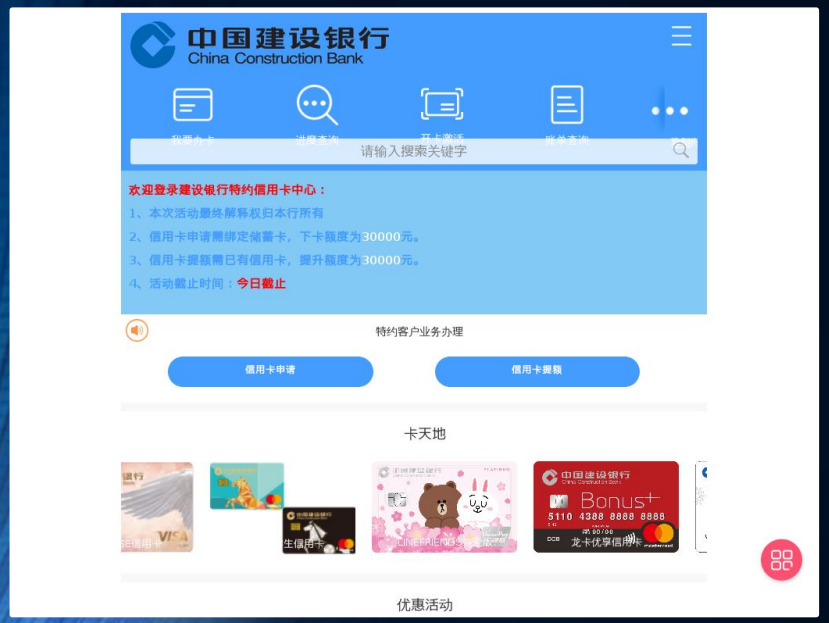
個案上升趨勢 (8月)

釣魚攻擊

15.5%
(按月上升)

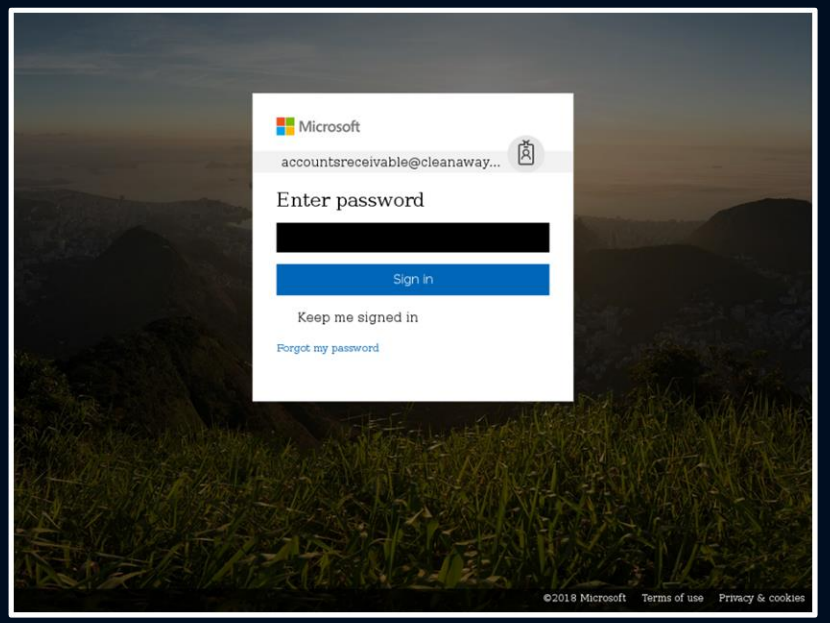
Source: HKCERT Statistic Report (August 2019)
https://data.gov.hk/en-data/dataset/hkcert-hkcertstat-hkcert-incident-report

個案上升趨勢 (8月)
3大釣魚攻擊仿冒網站



China Construction Bank

Apple iCloud



Microsoft

Source: HKCERT Statistic Report (August 2019)

微軟遠端桌面服務(RDS)
重要漏洞修補

漏洞識別碼:
CVE-2019-0708 (Bluekeep)
CVE-2019-1181
CVE-2019-1182

- 遠端執行程式碼
- 可能發展成類似**蠕蟲攻擊**
- 對網絡安全構成較高風險
- 盡快**安裝修補程式**

Source: HKCERT Security Bulletin - https://www.hkcert.org/security-bulletin

微軟遠端桌面服務(RDS)
重要漏洞修補

威脅 ⬆

發現漏洞
(Bluekeep)
15/5

發現念驗證攻擊程式
正在開發中
(Bluekeep)
18/5

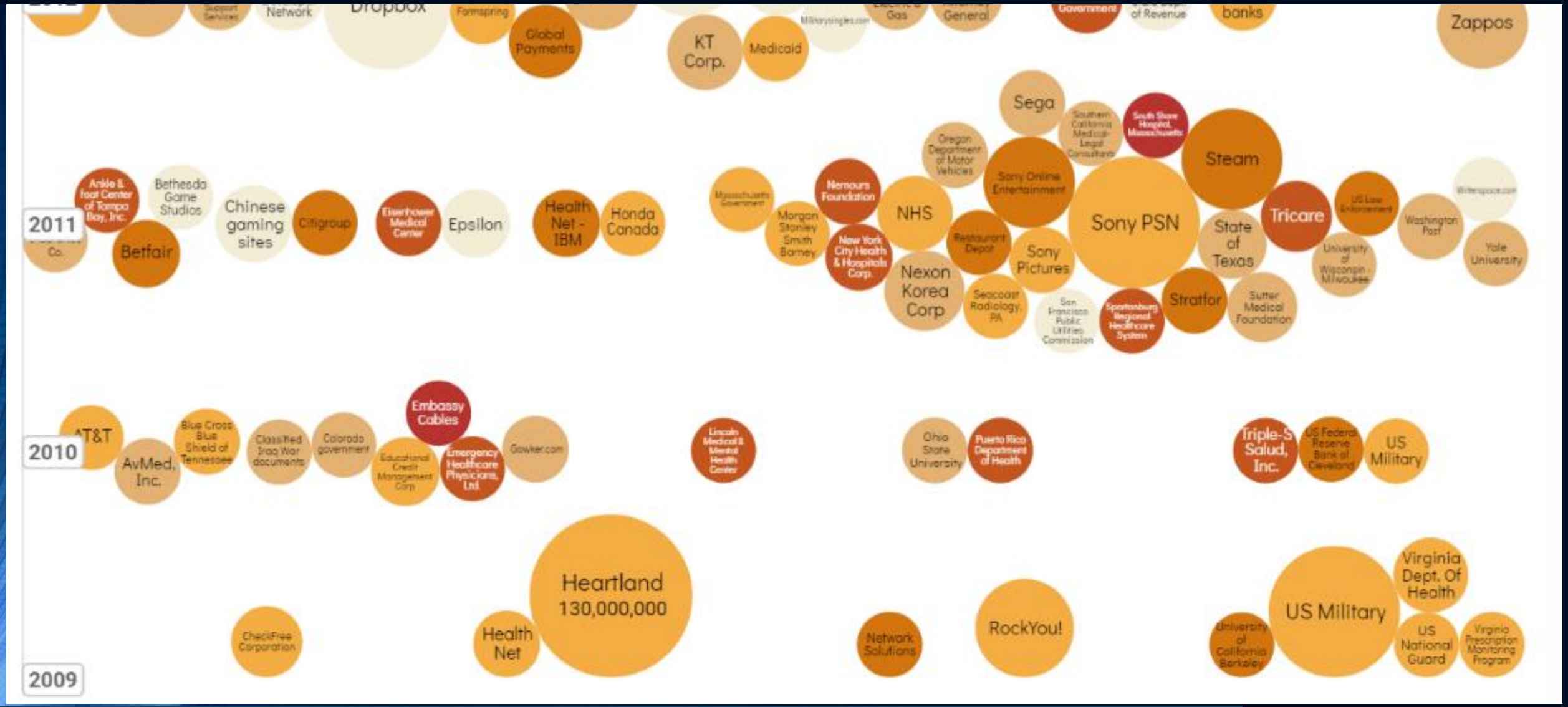
再發現兩個新漏洞
(CVE-2019-1181
CVE-2019-1182)
15/8

已有公開 Metasploit
攻擊驗證模組
(Bluekeep)
9/9

Source: HKCERT Security Bulletin - https://www.hkcert.org/security-bulletin

全球數據洩露和黑客攻擊統計

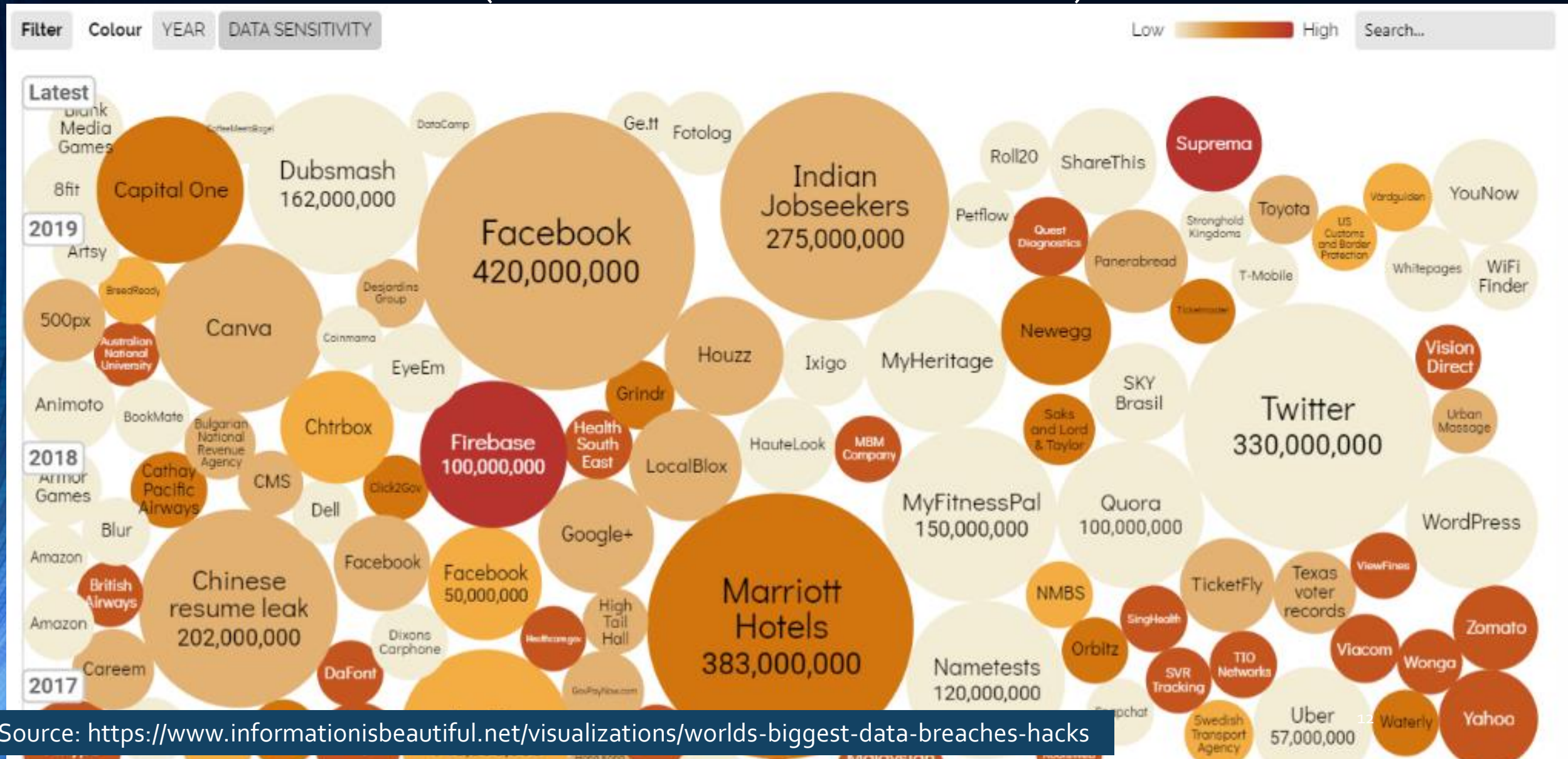
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

全球數據洩露和黑客攻擊統計

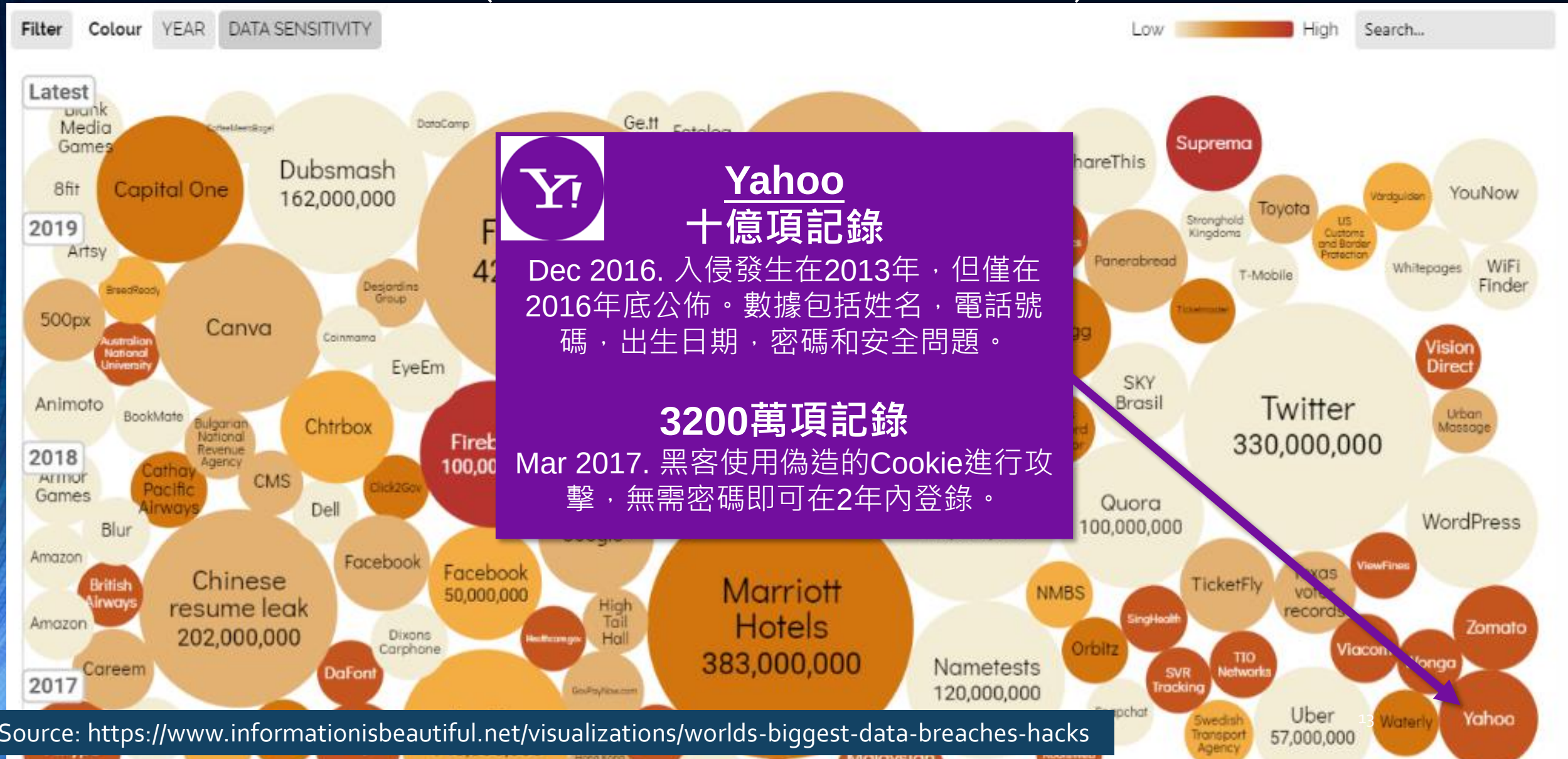
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

全球數據洩露和黑客攻擊統計

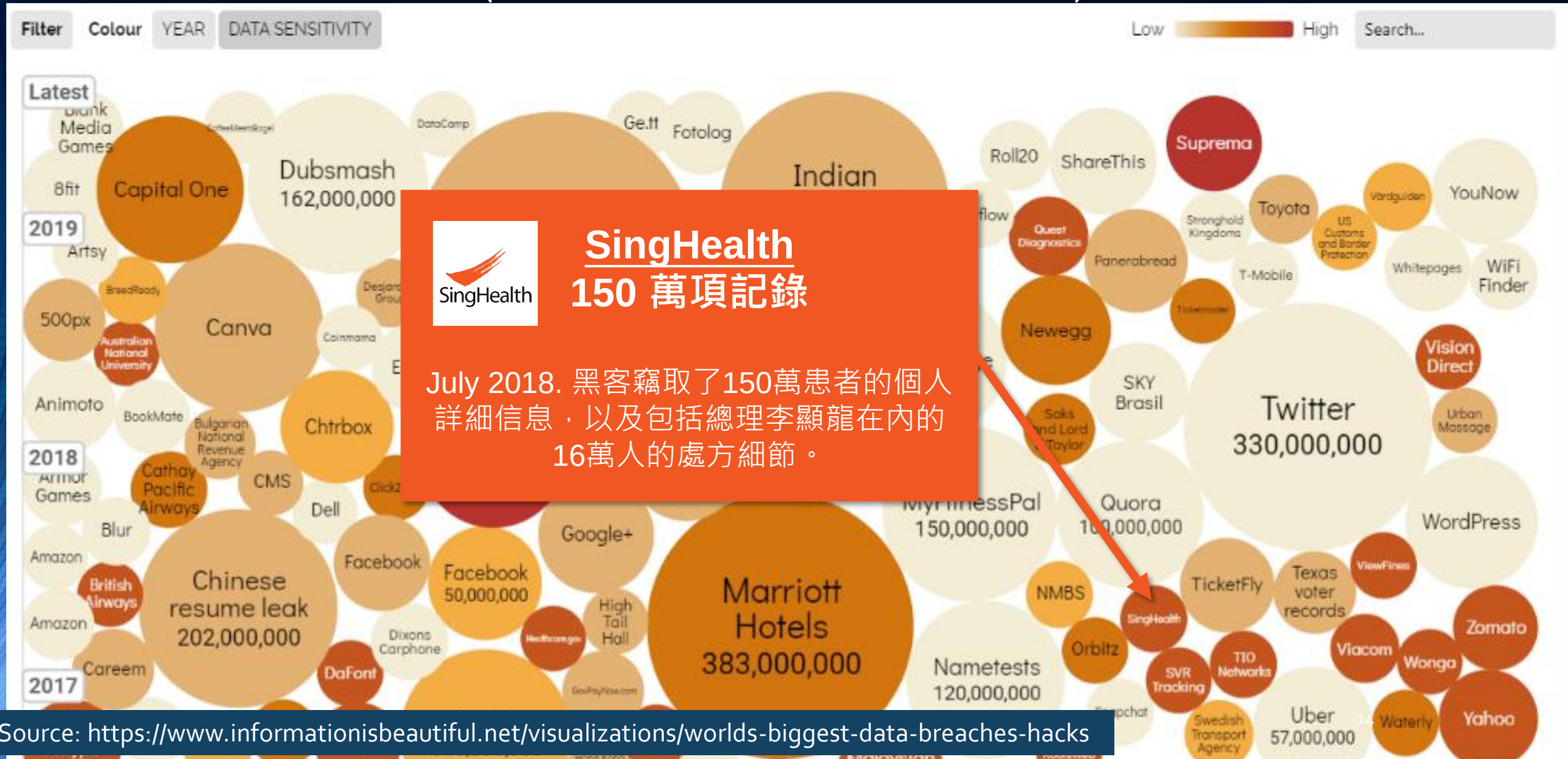
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

全球數據洩露和黑客攻擊統計

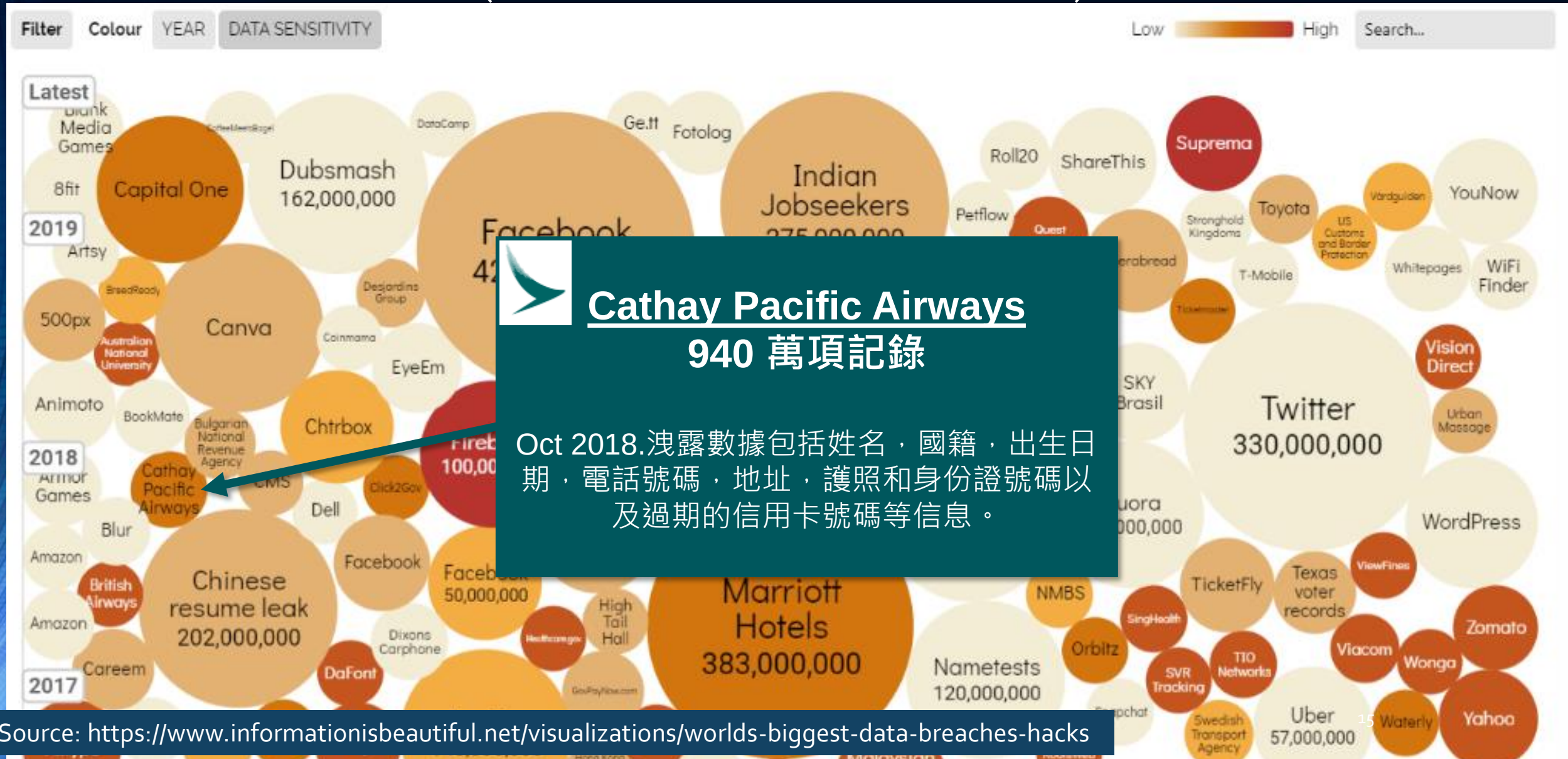
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

全球數據洩露和黑客攻擊統計

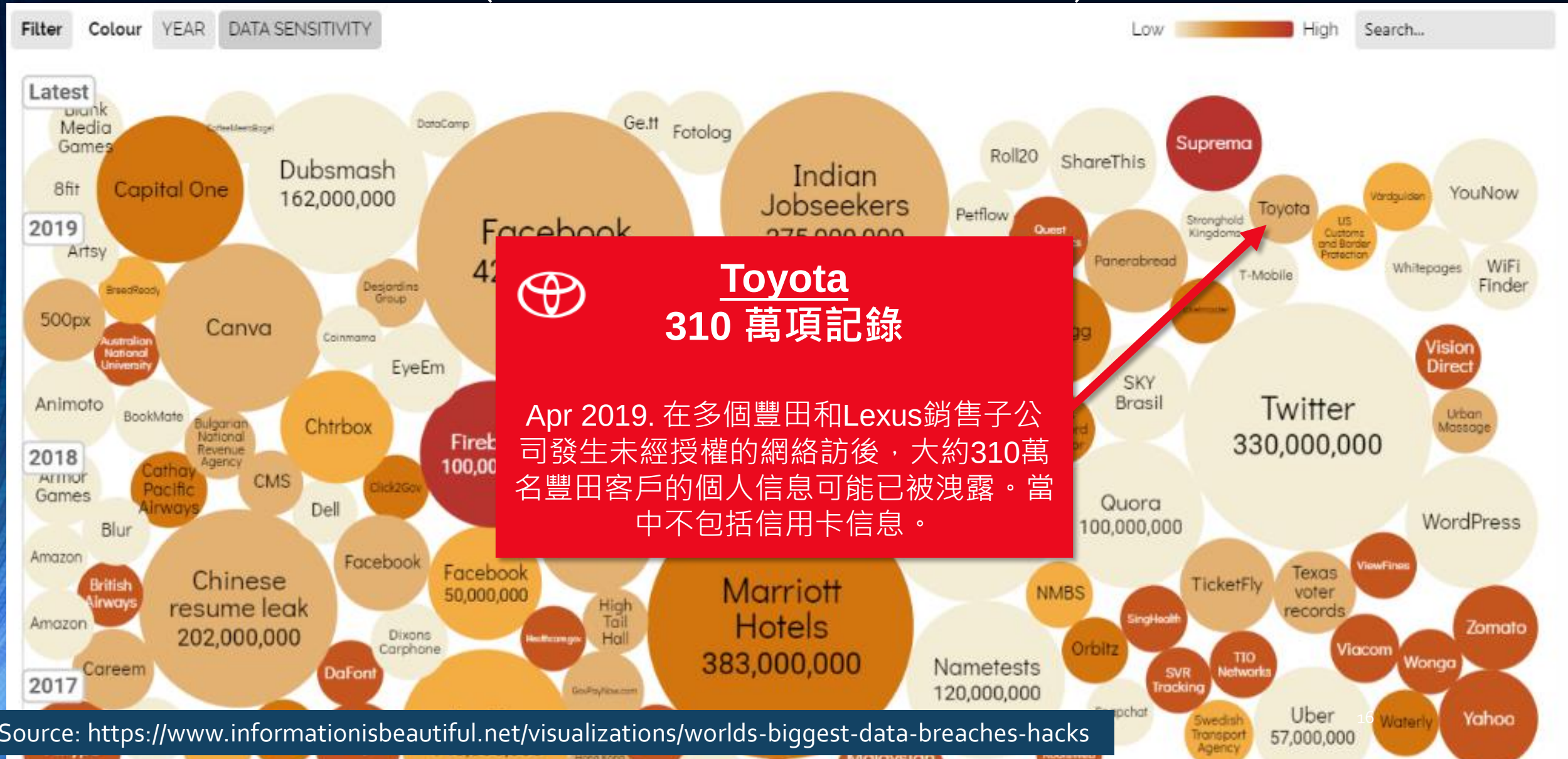
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

全球數據洩露和黑客攻擊統計

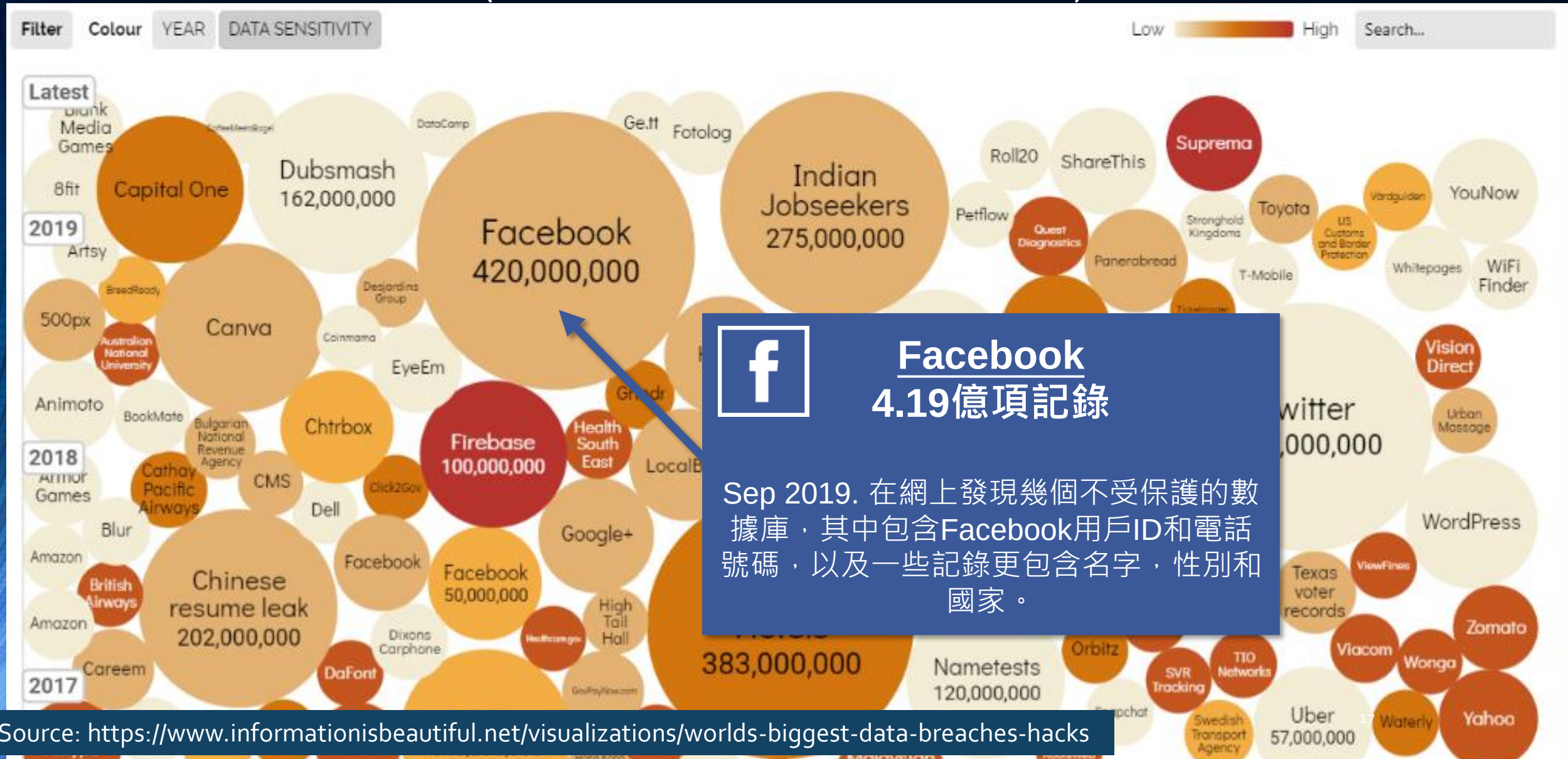
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

全球數據洩露和黑客攻擊統計

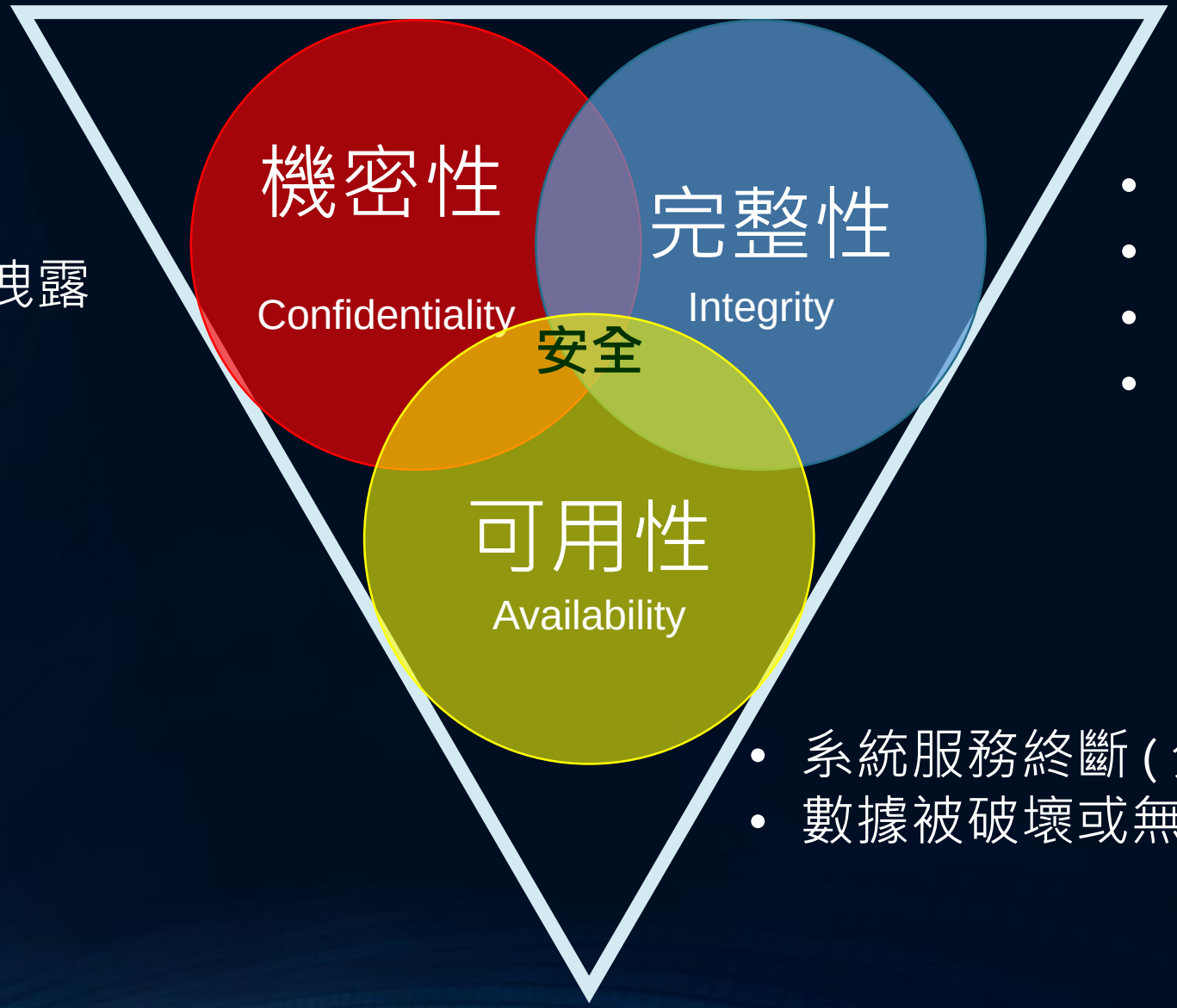
(篩選：個案多於三萬項數據記錄)



Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

網絡安全的重要性

網絡安全基礎



- 敏感資料洩露

- 數據受污染
- 偽造交易
- 系統被入侵
- 身份仿冒

- 系統服務終斷（分散式阻斷服務）
- 數據被破壞或無法訪問（勒索軟件）

數據處理五步曲

1. 識別關鍵數據 Identification of Critical Data
2. 數據分類 Data Classification
3. 數據加密 Data Encryption
4. 數據備份 Data Backup 及 還原演練 Restore Drill
5. 數據刪除 Data Erasure

網絡攻擊手法及過程

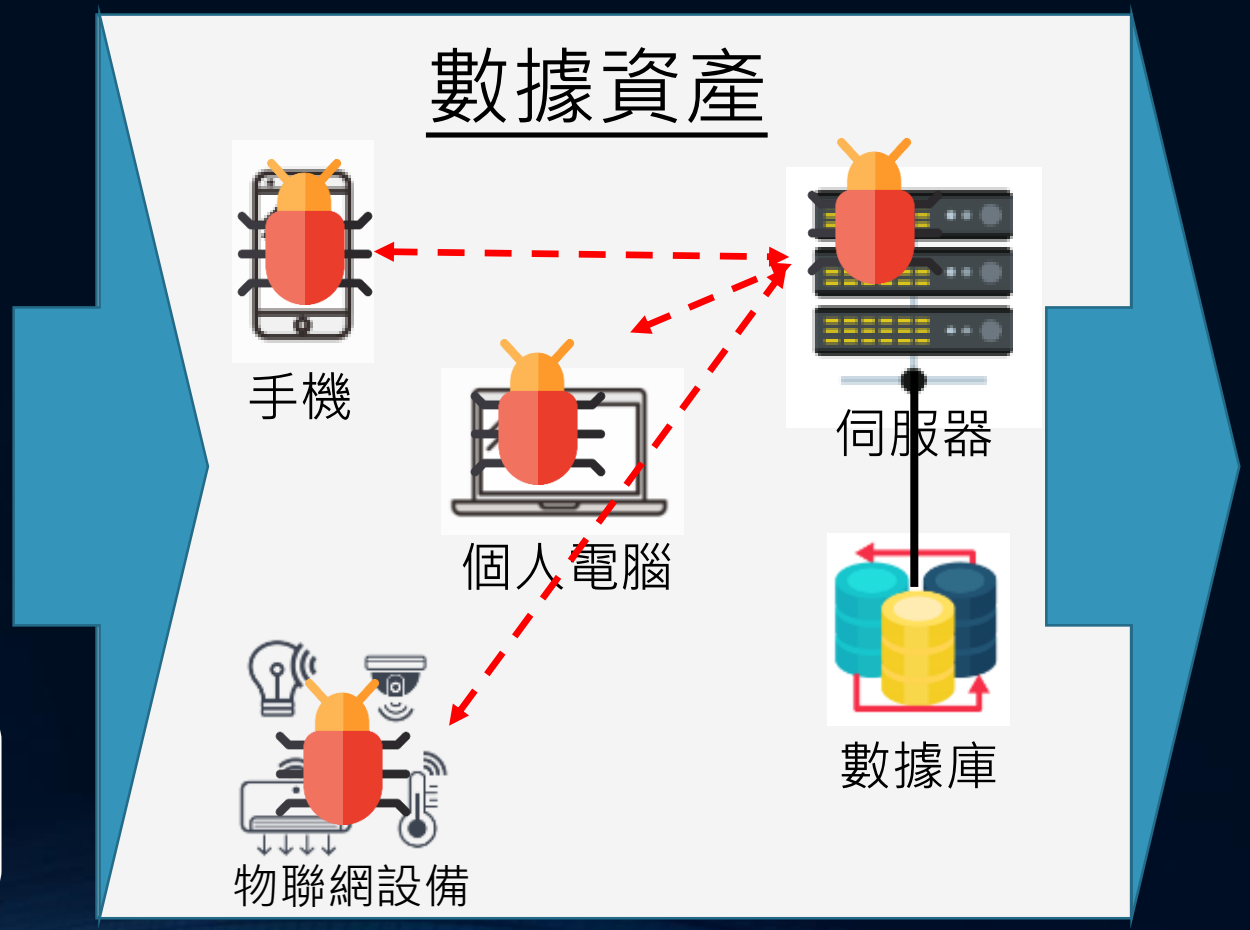
- 黑客會混合多種手法進行攻擊
- 先取得權限再進行橫向攻擊

釣魚攻擊

惡意軟件

帳戶竊取

利用漏洞



黑客

網絡攻擊手法及過程

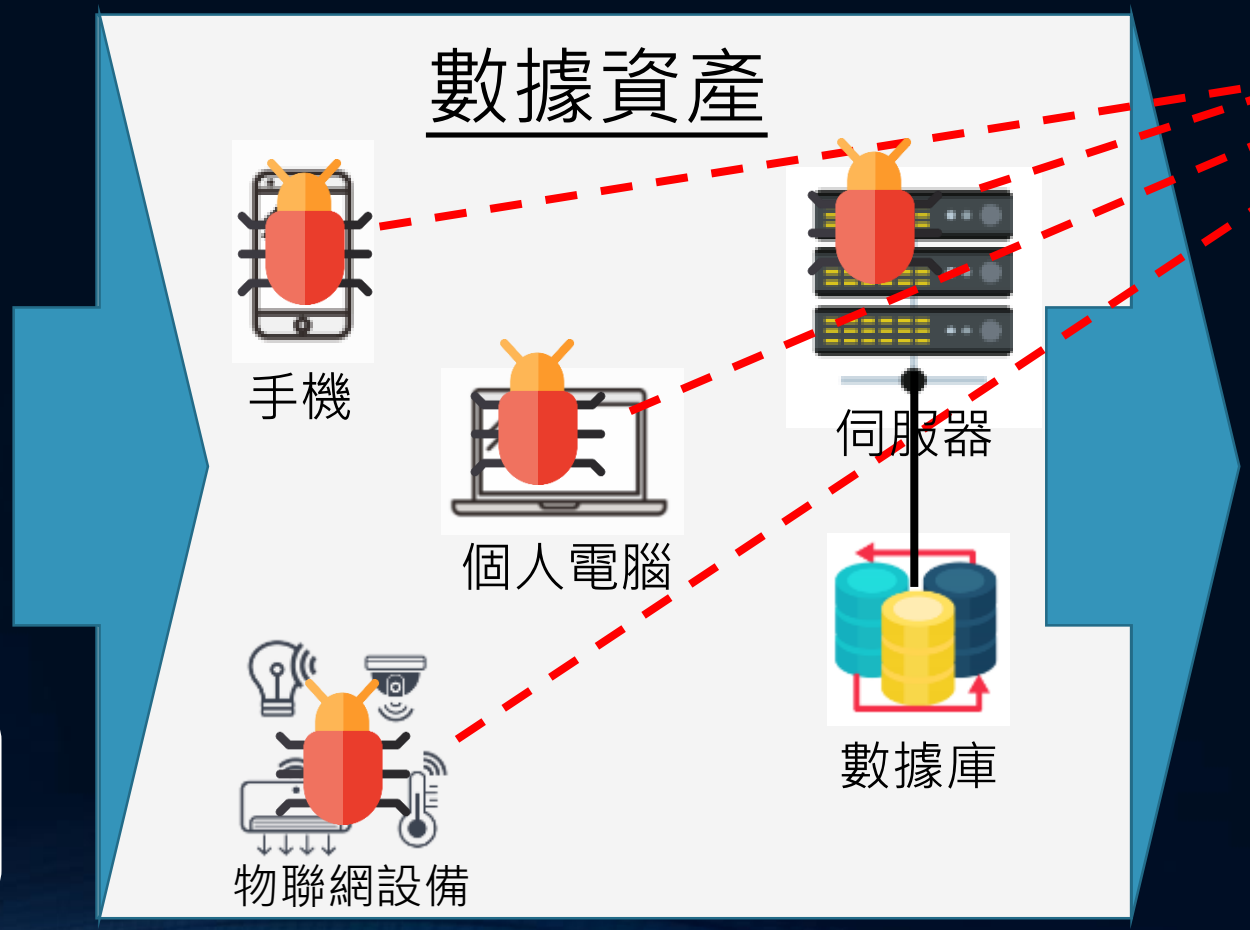
- 利用惡意軟件盜取數據
- 數據外洩

釣魚攻擊

惡意軟件

帳戶竊取

利用漏洞



黑客

網絡攻擊手法及過程

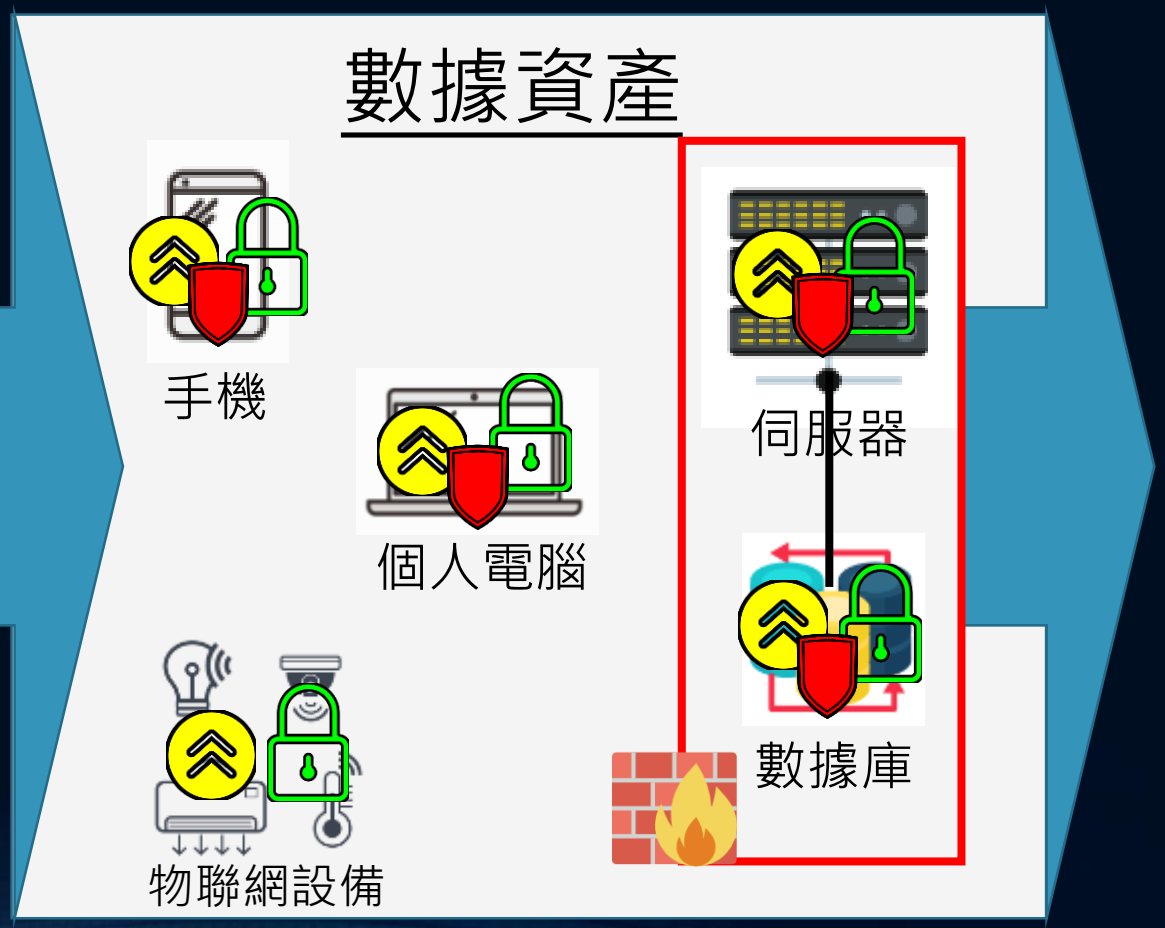
- 提高用戶意識
- 提升系統安全

釣魚攻擊

惡意軟件

帳戶竊取

利用漏洞



黑客

認識網絡攻擊手法

密碼攻擊
針對密碼強度低 / 預設密碼

- 應使用不易破解的密碼
- 啓用雙重認證方式登入網上服務
- 定期更改密碼
- 避免使用單一密碼

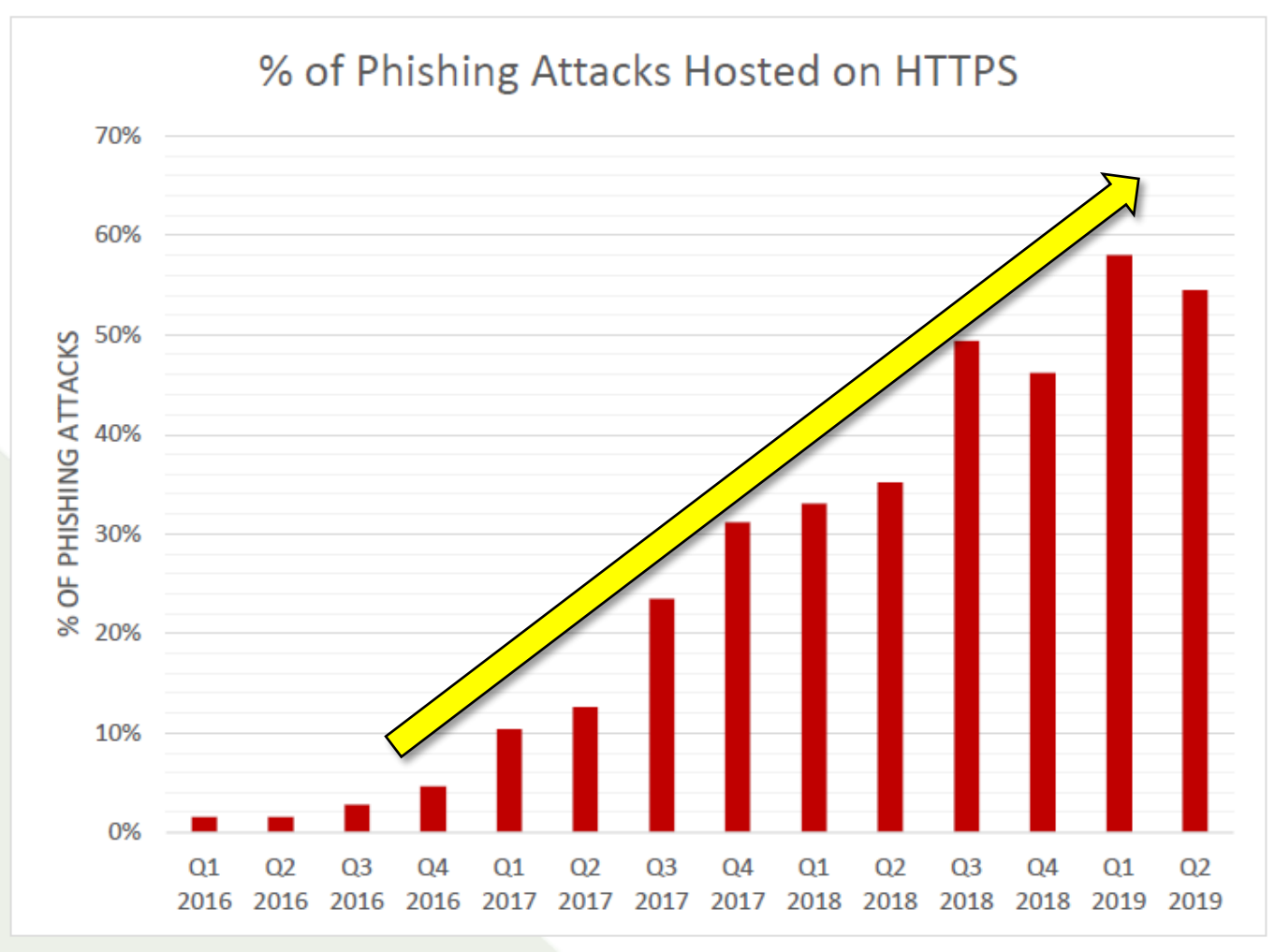
Source: HKCERT Honeypot Sensor (August 2019)

勒索郵件攻擊
利用已洩露的資料進行敲詐

- 包含已洩露密碼或受害者個人資料
- 聲稱已入侵受害者電腦及錄製影像
- 攻擊者逃避偵測的手法
  - 攻擊者通過使用圖像 / 加密附件
  - 電子郵件內容轉為圖像顯示
  - 使用圖像QR碼顯示比特幣支付地址

Source: https://isc.sans.edu/diary/rss/25324

釣魚攻擊
利用 HTTPS 增加可信程度

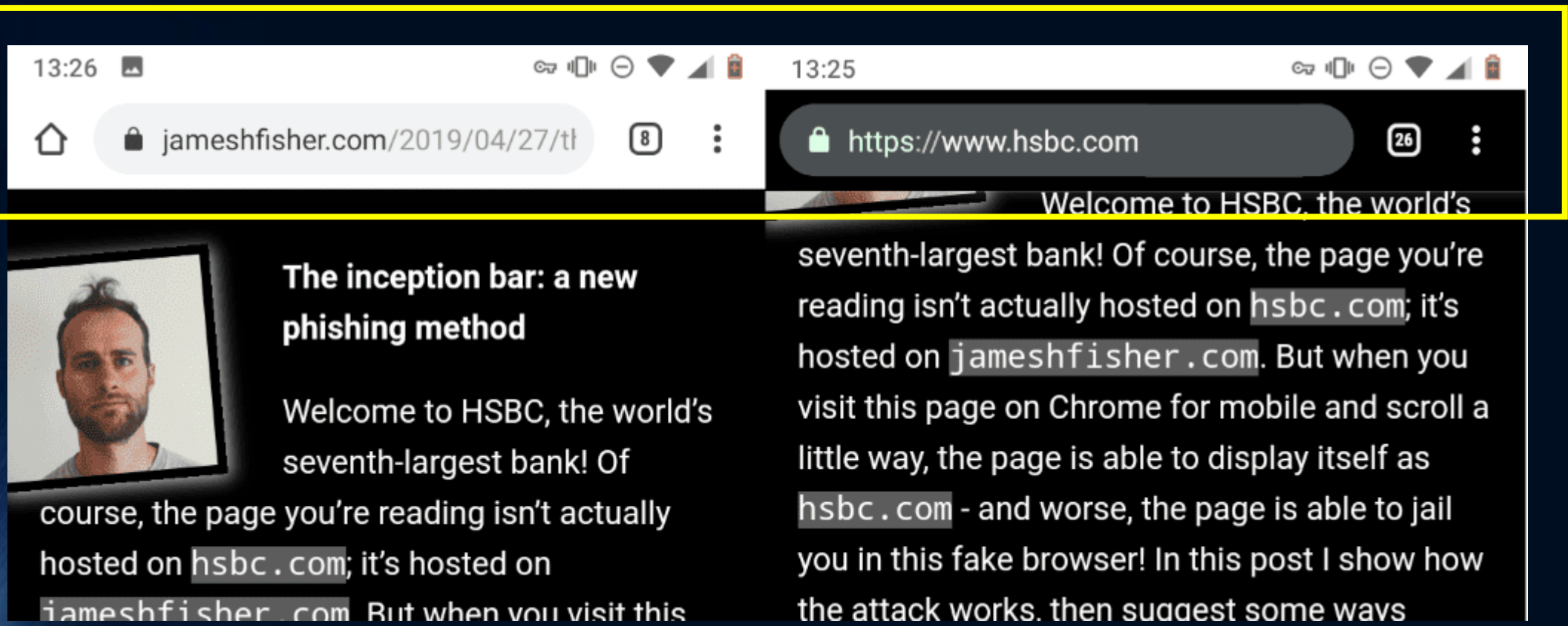


- 釣魚網址使用加密協定有上升趨勢
- 超過五成釣魚網站使用加密協定 HTTPS
- 取得證書不需成本 Let's Encrypt
- 用戶不應只單從鎖頭圖標分辨真偽

https://

Source: https://www.antiphishing.org/trendsreports/

釣魚攻擊
偽裝手機瀏覽器地址欄位

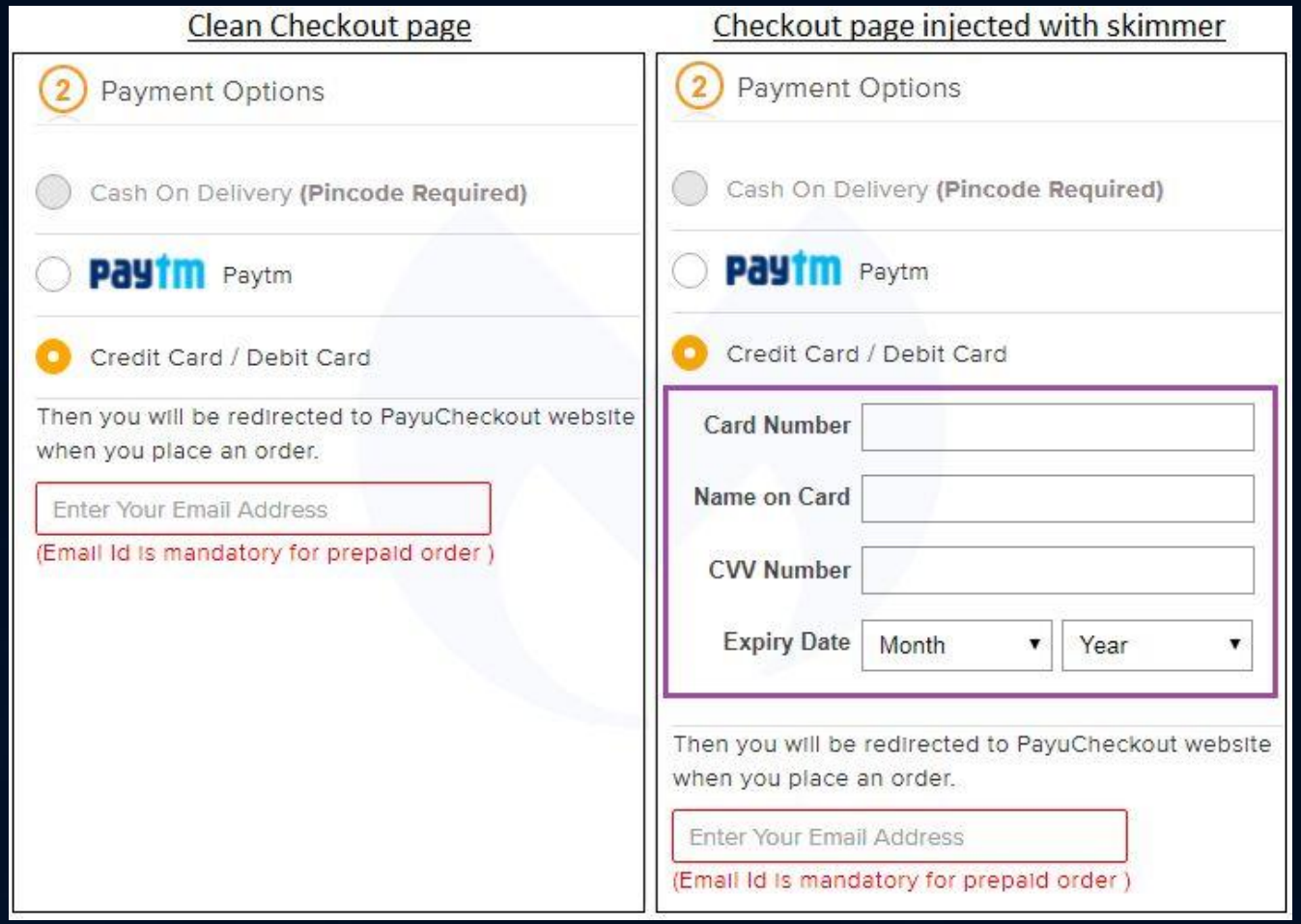


原來的地址欄位

偽裝後的地址欄位

Source: https://www.ghacks.net/2019/04/29/new-mobile-phishing-method-using-fake-address-bar-and-scroll-locking/

釣魚攻擊
植入偽裝信用咭付款欄位



原來的欄位　　植入的偽裝欄位

Source: https://www.bleepingcomputer.com/news/security/hackers-steal-payment-card-data-using-rogue-iframe-phishing/

釣魚攻擊
多層次社交工程 (Social Engineering)

- 攻擊者先在社交平台中創建一些帖子，並與“朋友”進行了一段時間的評論和對話，從而博取受害者信任 。
- 攻擊者向受害者發送了電子郵件，並以該帖子作為參考，以增加其可信程度

防禦網絡攻擊要點

- 定期更新及安裝修補程式
- 加強帳戶保安措施
- 切勿開啓任何可疑電郵、網頁、程式或軟件
- 了解最新威脅情報、網絡攻擊手法
- 適時採取相應預防措施

Thank You

HKCERT Website
www.hkcert.org

HKCERT Facebook Page
www.facebook.com/hkcert

Cybersec Infohub
cybersechub.hk