新生醫專
網路資訊安全

簡報人員：忠明

簡報單位：精誠軟體服務

技術協助單位：三勝資訊

精誠軟體服務
SYSTEX Software & Service

Agenda

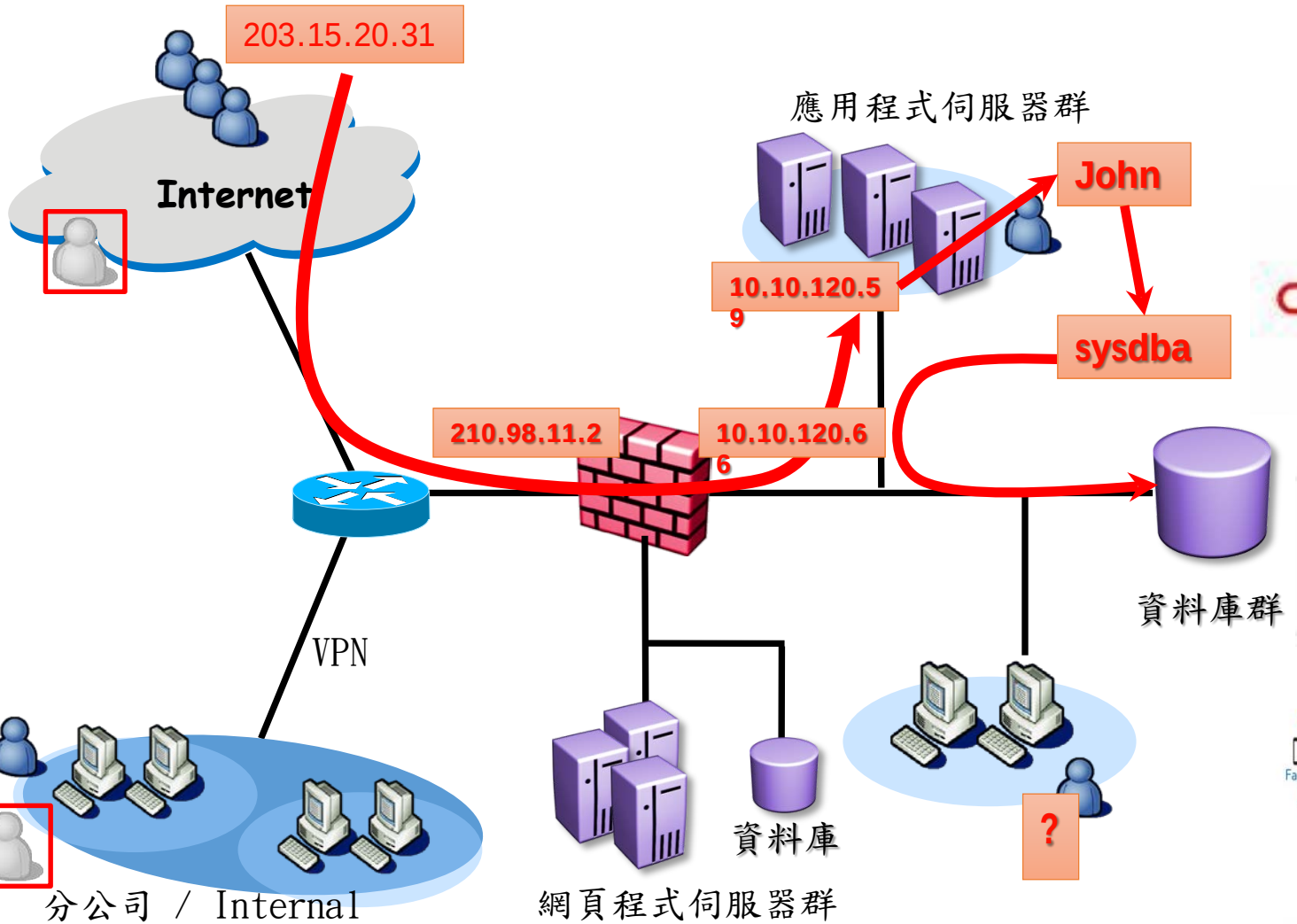
- 網路資訊安全概述
- 2016重大網路資安事件說明
- 行動網路資訊安全說明
- 簡易網路資安演練
- 影片觀賞
- QA

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述


petabytes
volume
Facebook
Media
Expert
Leader
programming
Effective
Devices
SOCIAL
VISUALIZATION
productivity
data mining

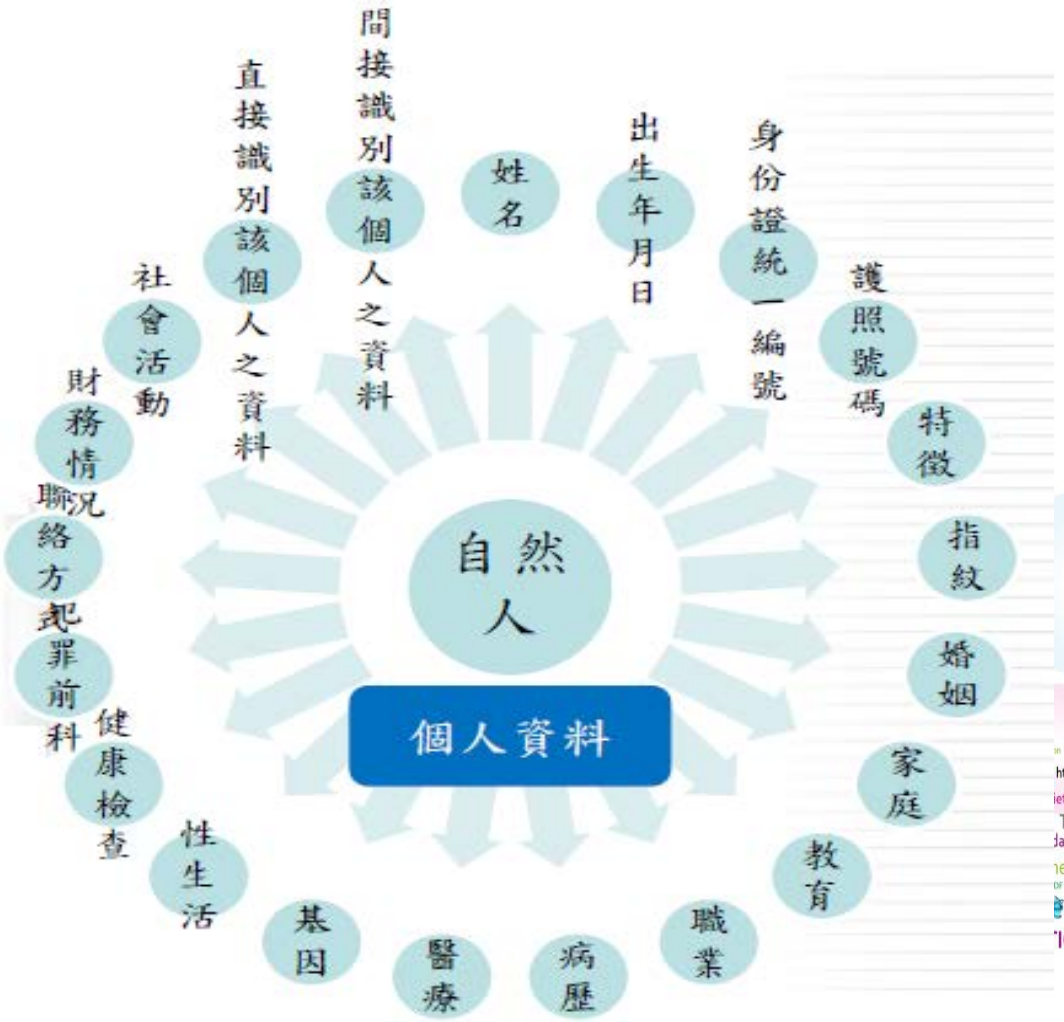
網路資訊安全概述－網路元件



網路資訊安全概述－個資

個人資料檔案：

依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合



網路資訊安全概述－個資

違反個資法致侵害當事人權利者，民事賠償每人每一事件

每人每一事件新台幣五百元以上，二萬元以下

被害人不易或不能證明其實際損害額時

同一原因事實造成多數當事人權利受侵害，合計賠償總額

新台幣二億元為限

該原因事實所涉利益超過新臺幣二億元者以該所涉利益為限

第41~43條

違反.....或中央目的事業主管機關依第21條限制國際傳輸之命令或處分，足生損害於他人者，**處二年以下有期徒刑、拘役或科或併科新臺幣二十萬元以下罰金**

意圖營利犯前項之罪者，**處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金**.....

第44條

公務員假借職務上之權力、機會或方法，犯本章之罪者，**加重其刑至二分之一**

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

- Ransomware:
  Your Money or Your Data

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

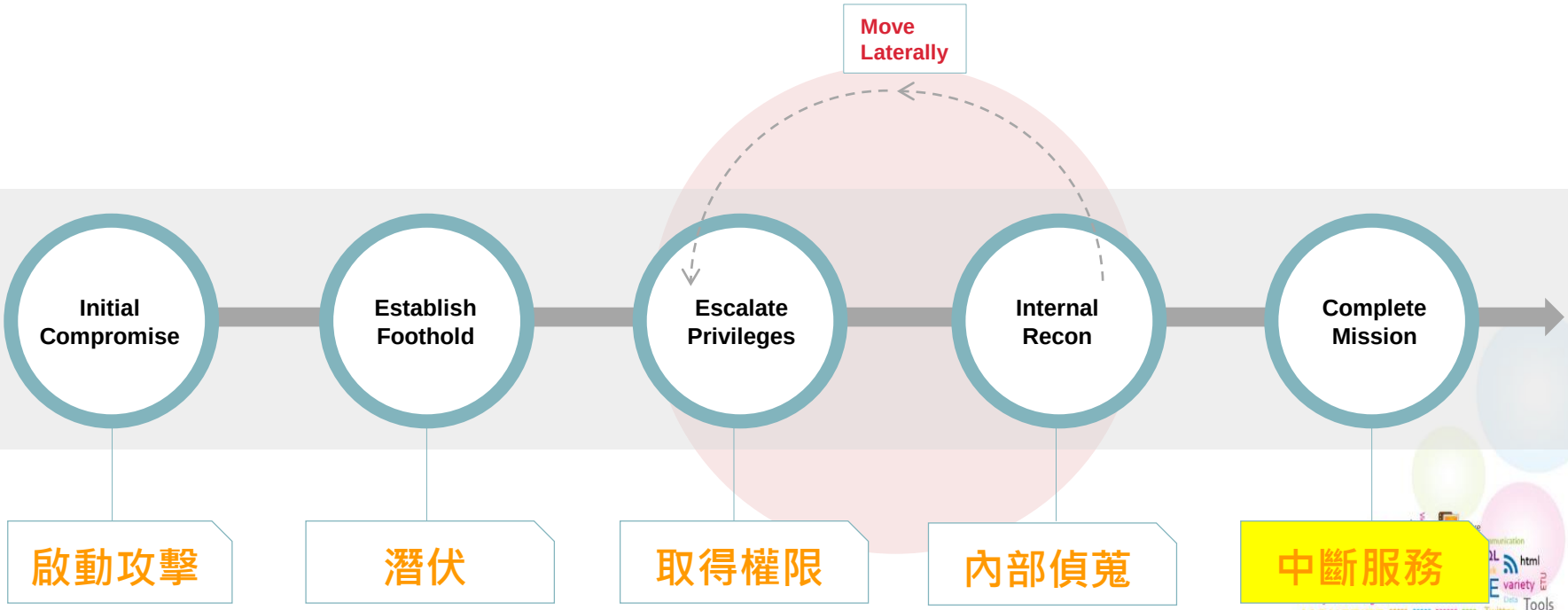
- NOT ALL THREAT ACTORS ARE THE SAME

	Nuisance	Hacktivism	Crime	Espionage	Warfare
Objective	 **Access & Propagation**	 **Defamation, Press & Policy**	 **Financial Gain**	 **Economic, Political Advantage**	 **Disrupt Operations**
Example	Botnets & Spam	Website Defacement	Credit Card Theft, Ransomware	Advanced Persistent Threats	Destroy Critical Infrastructure
Targeted	☒	☑	☑	☑	☑
Character	Automated	Conspicuous	Opportunistic	Persistent	Conflict-driven

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體



精誠軟體服務
SYSTEX Software & Service

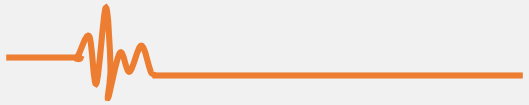
網路資訊安全概述 – 複合型態威脅模式

Ransomeware 勒索軟體

夾帶惡意檔案，
搭配社交工程
手法攻擊

量身打造的攻擊

長期潛伏不易察覺



惡意檔案多透過
文件格式檔案包裹

鎖定目標攻擊

組織型駭客攻擊 | 魚叉式攻擊 | 精準式攻擊 | 目標式攻擊 | 社交工程攻擊

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

電子郵件：
釣魚郵件、惡意夾檔

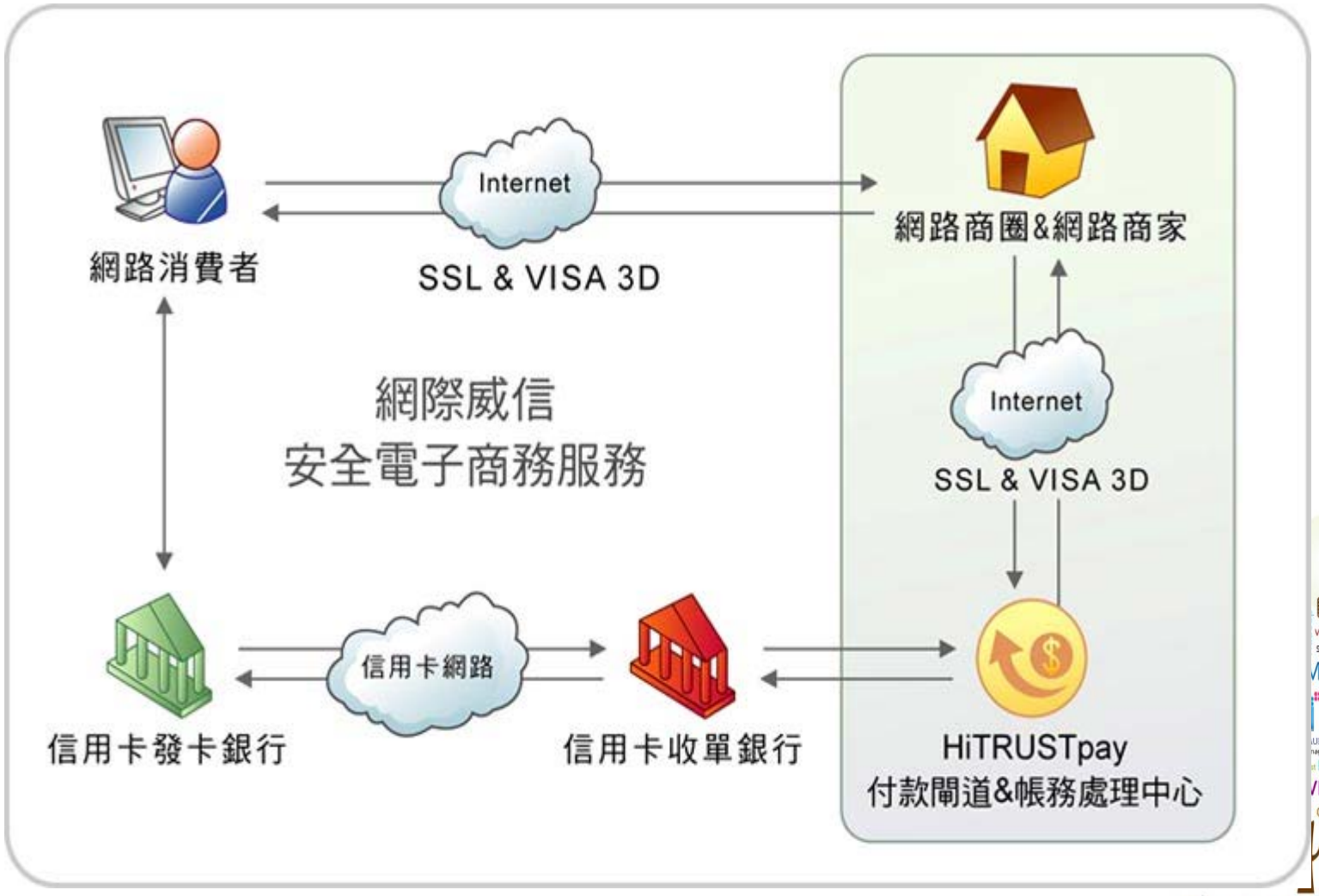
- 假冒銀行或快遞，連結下載帳單或收據
- 偽裝成投履歷或寄送發票的信件
- 夾帶惡意檔案，解壓縮後是勒索軟體

網際網路：
釣魚網站、惡意廣告

- 連到釣魚網站，透過瀏覽器(IE)對Flash外掛等進行攻擊
- 勒索軟體假裝網頁廣告，點擊就中獎
- 隱藏在外觀正常的網站，植入惡意程式與連結

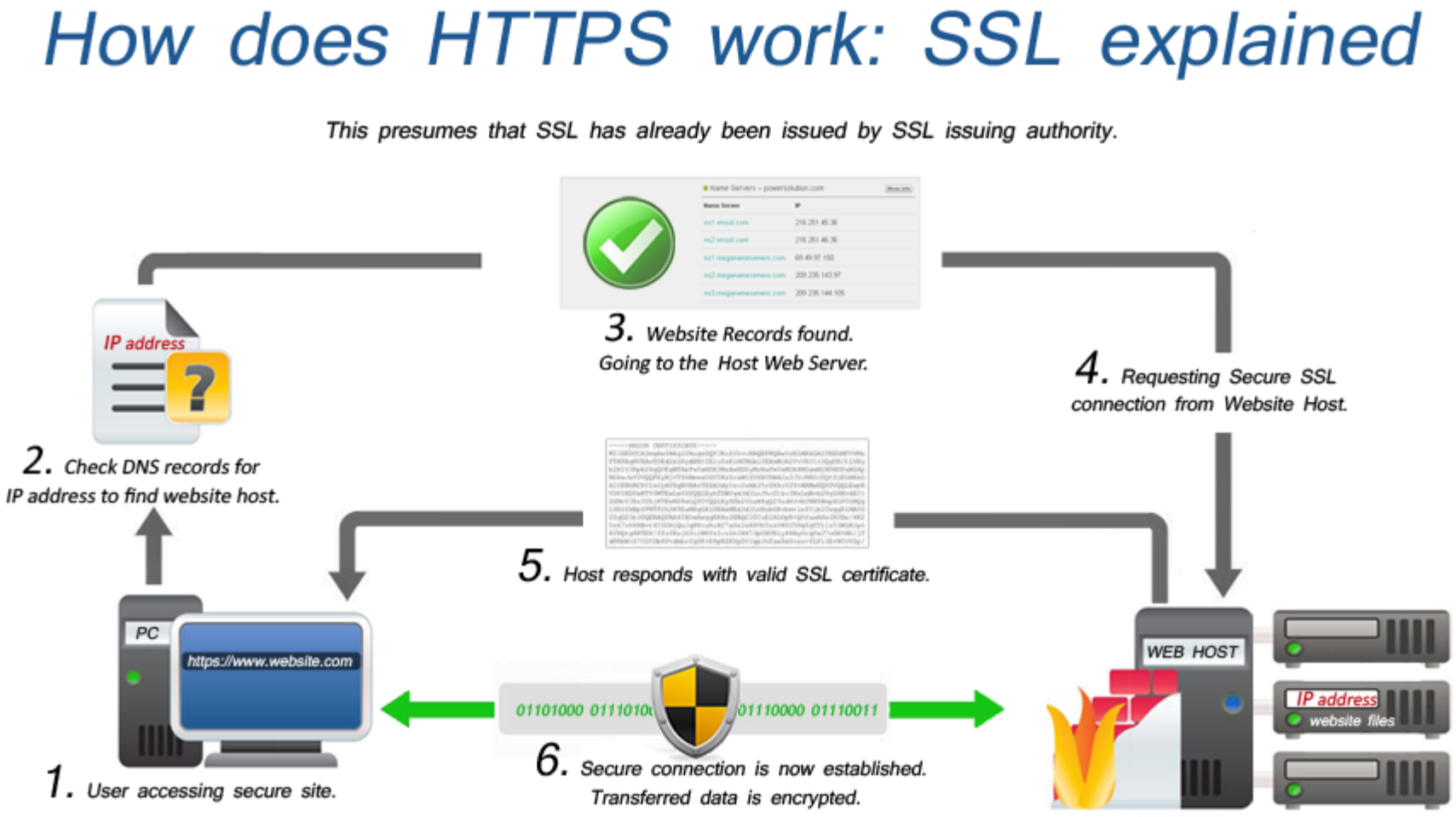
精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－網路交易平台



精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－網路交易平台



精誠軟體服務
SYSTEX Software & Service

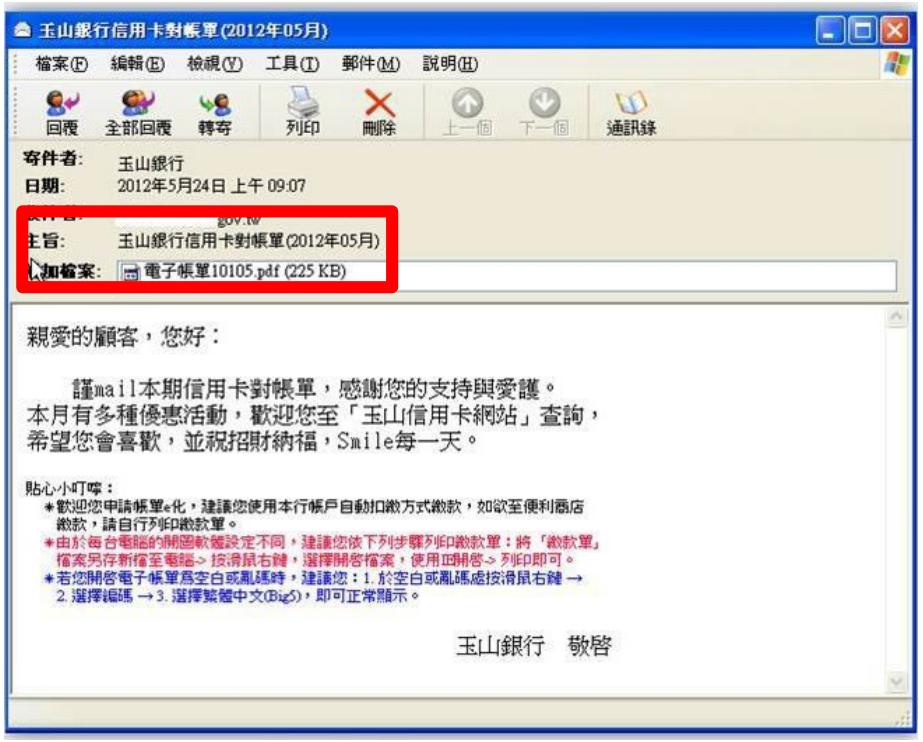
網路資訊安全概述－網路交易平台

「第三方支付」交易流程

狀況處理：買家收到商品，若在商品鑑賞期內，對商品不滿意，或認為與賣家承諾有出入，可向第三方支付平台提出異議，並將貨物完整退回賣家。第三方支付平台確認賣家收到退貨無誤後，將退款還給買家。若買賣雙方對以上處理沒有共識，則由其中一方提交法院進行協調與判決，第三方支付平台再依判決內容，確認退款買家或撥付給賣家的金額。

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體



精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

udn / 即時 / 社會

相關新聞

嘉義城隍廟電腦被加密 歹徒寄信勒索比特幣

分享 | G+ 分享 | 留言 | 列印 | 存新聞 | A- A+

2016-07-20 23:15 聯合報 記者魯永明／即時報導 讚 489 分享 傳送 G+1 0

國外勒索軟體橫行，不少商家、民眾受害，連國定古蹟嘉義城隍廟也遭殃。城隍廟電腦硬碟資料被加密，勒索近兩萬元，電腦內建廟三百周年、建國百年全國城隍大會師等資料「統統不見了」，連珍貴的清朝建廟碑文也找不到，「災情」慘重。

「咦！怎麼搞的，檔案都打不開」，嘉義城隍廟總幹事葛永樂手按滑鼠，上雅虎奇摩網站瀏覽，同時想點開文書系統工作時，發現資料檔案被加密，打不開，心急如焚。不久就收到一封英文郵件，勒索相當台幣兩萬的「比特幣」贖金。

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

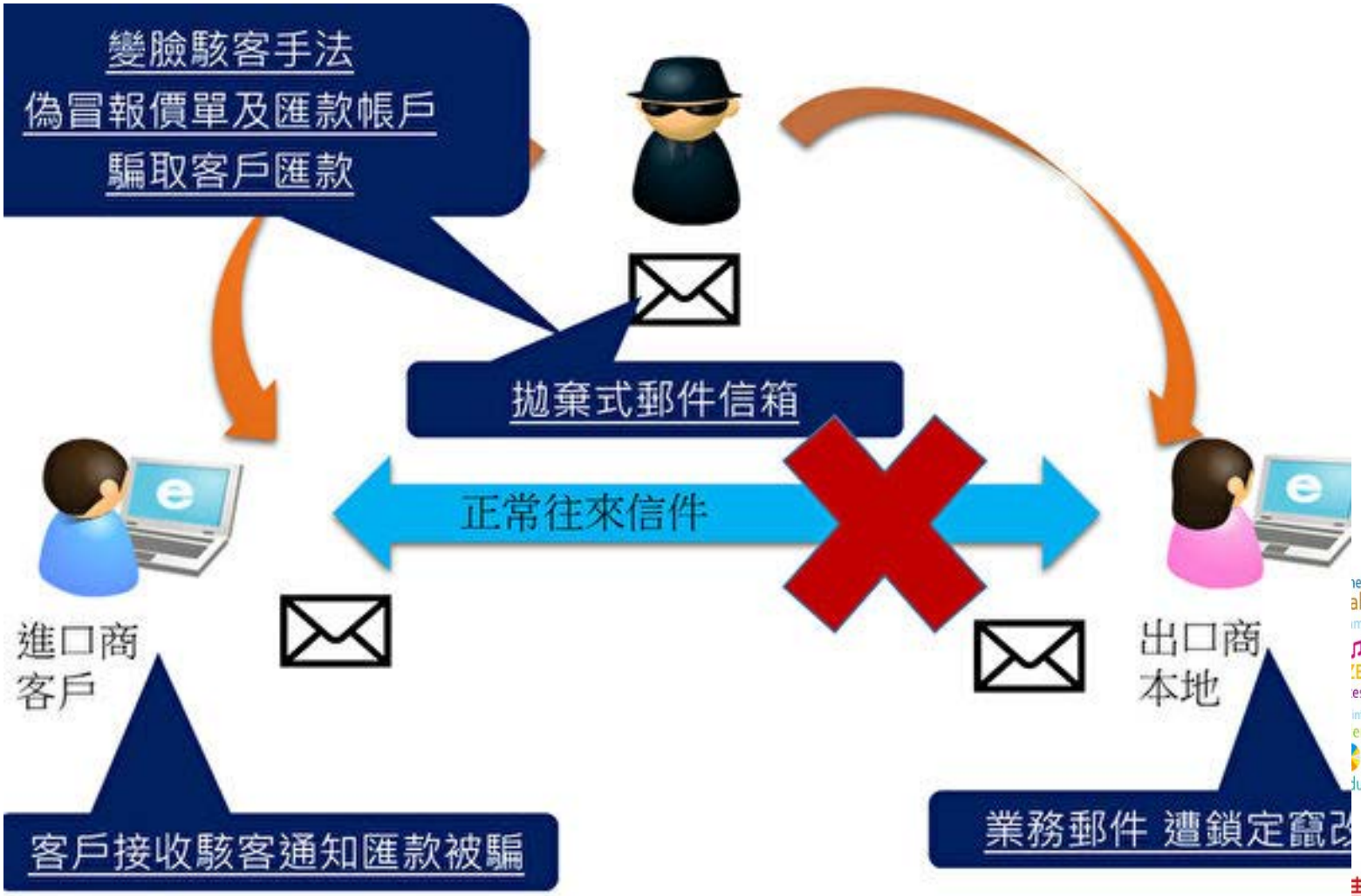
*"**Ransomware** is a type of malware that restricts access to the infected compute system in some way, and demands that t user pay a ransom to the malware opera to remove the restriction."*

WIKIPEDIA

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體



網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

阿拉伯數字 0

大寫英文字母 O

網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

https://member.ruten.com.tw/user/login.htm 真

http://member-ruten.com.tw/user/login.htm ;
http://members-ruten.com/user/login.htm

網址差異不大
真假不易分辨

https://login.yahoo.com/config/mail?.intl=tw 真

https://login-yahoo.com/config/mail?.intl=tw

SOCIAL intelligence VISUALIZATION
productivity data mining

精誠軟體服務
SYSTEX Software & Service

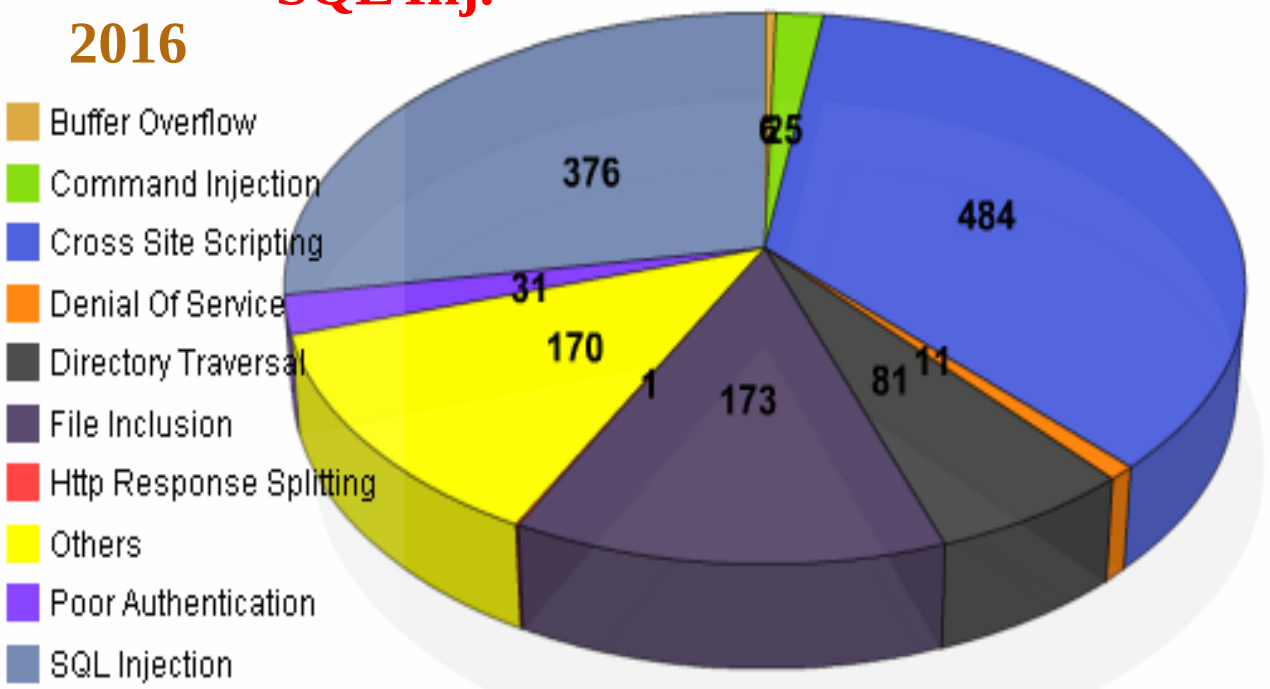
網路資訊安全概述－複合型態威脅模式

Ransomeware 勒索軟體

網路資訊安全概述 – AP / Web 攻擊模式比例

SQL Inj.

2016



XSS

資料來源: CVE (Common Vulnerability Enumeration)
http://cve.mitre.org

4

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述 – SQL Injection

```
SELECT * FROM user_db
WHERE ID = '&Request("ID")&' AND
      PWD = '&Request("PWD")&';
```

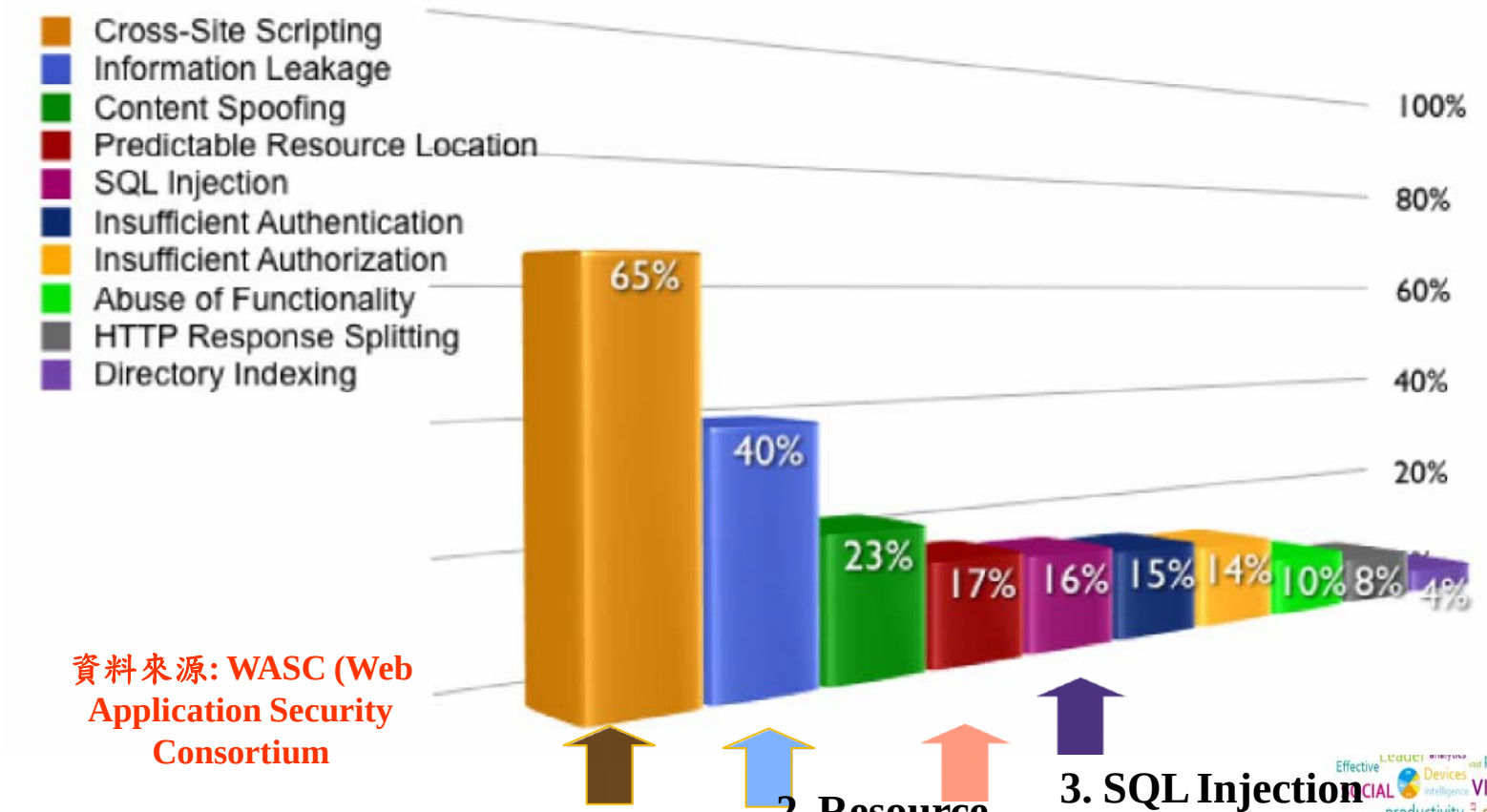
ID = '' OR 1=1 -- '

PWD = 'ooxx'

```
SELECT * FROM user_db
WHERE ID = '' OR 1=1 -- '' AND
      PWD = 'ooxx';
```

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述 – AP / Web 攻擊模式比例



資料來源: WASC (Web Application Security Consortium

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－網頁漏洞測試

- **黑箱測試 (Blackbox Testing)**
  - 在受測目標資訊不足的情況下進行測試，例如主機資訊、系統設定、 原始碼等等
  - 由於測試重複性高，多採用自動化工具協助
  - 如：弱點掃描、滲透測試

- **白箱測試 (Whitebox Testing)**
  - 在取得受測目標資訊的情況下進行測試
  - 由於資訊充足，常以檢查及驗證為主
  - 過去缺乏自動化工具，現已有成熟工具可協助
  - 如：Code Review、源碼檢測

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－資安防護重點

精誠軟體服務
SYSTEX Software & Service

網路資訊安全概述－資安防護重點

2016重大網路資安事件說明

2016重大網路資安事件說明

- **駭客入侵一銀ATM**

結果： 臺北、臺中22家第一銀行分行內41臺ATM 吐鈔盜走了8,327萬7,600元

駭客團隊：來自東歐-俄羅斯黑幫 / 拉脫維亞籍洗錢嫌犯安德魯

精誠軟體服務
SYSTEX Software & Service

2016重大網路資安事件說明

- 駭客入侵一銀ATM

2016重大網路資安事件說明

- **駭客入侵一銀ATM**

駭客從遠端登入，開始將木馬程式派送到ATM設備中，包括了控制ATM遠端吐鈔程式cngdisp.exe及cngdisp_new.exe

顯示受駭ATM資訊的惡意程式cnginfo.exe

一個批次檔cleanup.bat，可用來執行微軟內建加密刪除工具sdelete.exe銷毀所有木馬程式。

精誠軟體服務
SYSTEX Software & Service

2016重大網路資安事件說明

- **駭客入侵一銀ATM**

駭客首先入侵的是個人電腦

從APT（進階持續性威脅），駭客有可能透過魚叉式釣魚郵件的方式，
騙取倫敦分行行員點選連結，下載木馬軟體，
入侵其個人電腦後取得進入內網的能力。

精誠軟體服務
SYSTEX Software & Service

簡易資安演練

簡易資安演練

- 測試自己的電腦環境
- IPConfig
- Ping
- Traceroute
- Netstat
- Nslookup

精誠軟體服務
SYSTEX Software & Service

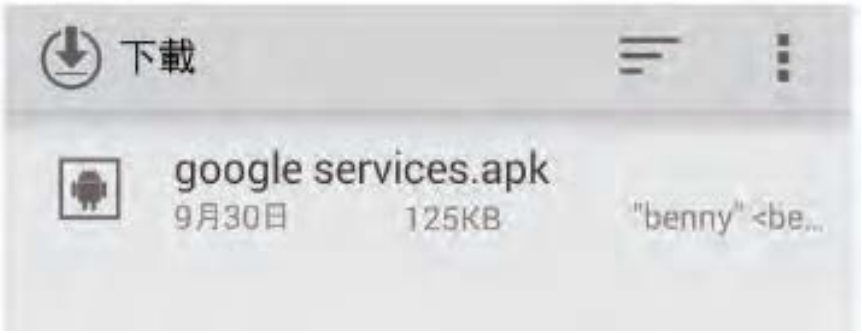
行動網路資訊安全說明

行動網路資訊安全說明

常見的手機漏洞

Android 系統智慧型手機：

請檢查手機"下載功能"，是否含有*.apk檔案



有害軟體名稱 (範例)	受影響裝置
com.fone.player1	Galaxy Note 2 LG G4
com.lu.compass	Galaxy S7 Galaxy S4
com.kandian.hdtogoapp	Galaxy Note 4 Galaxy Note 8.0
com.sds.android.ttpod	Galaxy Note 2 Xiaomi Mi 4i
com.baycode.mop	Galaxy A5
com.kandian.hdtogoapp	Galaxy S4
com.iflytek.ringdiyclient	ZTE x500
com.android.deketv	Galaxy A5

被植入「後門」的手機會主動傳送用戶與裝置資訊，
包括「訊息全文、聯絡簿、附完整電話號碼的通話紀錄」

行動網路資訊安全說明

手機晶片漏洞

Apple /Android系統智慧型手機：
博通Wi-Fi晶片Broadpwn漏洞

能夠捕獲目標設備所發出的Wi-Fi探測請求，
並將該設備引導至惡意Wi-Fi熱點上，
允許駭客傳遞數據以摧毀Wi-Fi晶片上內存，
卻完全不驚動使用者

原文網址：https://kknews.cc/zh-tw/tech/og354pp.html

行動網路資訊安全說明 - 影片觀賞

Time 17:55
Hacking the Smartphone | Mobile Cyber Hack Demonstration | Mobile Security
https://youtu.be/Tn2etDAul98

Time 22:00
詳解比特幣原理和運行機制
https://youtu.be/P4seQcP77H4

Time 10:00
Very simple way of hacking the "keyless entry" system of modern cars
https://youtu.be/1Z2x6L9sV3Q

精誠軟體服務
SYSTEX Software & Service

Thank You !

Q & A

精誠軟體服務
SYSTEX Software & Service