惡意程式攻防
與數位鑑識分析

Jimmy Hsu
winterthink@gmail.com

自我介紹

學歷	元智大學資訊管理學系 政治大學資訊科學研究所
經歷 (共19年)	元智大學資管系兼任講師 銘傳大學資管系兼任講師 恆逸教育訓練中心講師 顧問服務業 鑑識實驗室副理 系統整合商 系統維運組長、專案經理
資安證照	EnCE, MCFE ,CCPA, CEH, CHFI, CEI, CSA, ECIH, CND, 17025
現職	新北刑大科技偵查專業顧問(2025) 政治大學資科系兼任助理教授(2023/9~現今) Magnet 原廠特約講師暨Influencer (2020~現今) EC-Council 原廠認證講師(2020~現今) 金融研訓院菁英講座 (2020~2023) 長庚大學資管系兼任助理教授(2017/1~現今) EnCase 原廠認證講師 (2006~現今)
擅長領域	數位鑑識、駭客攻防、滲透測試、弱點掃描、ISO 17025、ISO 17043、ISO 27001、ISO 20000、資訊機房管理
授課/ 專案經驗	• 台灣銀行、中央銀行、富邦銀行及中華郵政 等金融業 • 中國人壽、全球人壽、新光人壽及宏泰人壽 等壽險業 • 法務部、調查局、中研院、高檢署及考試院 等政府機關 • 國防部、憲指部、陸總、資通電軍及軍情局 等軍方機關 • 警政署科技犯罪組、刑事局及各縣市警察局 等治安機關 • 台灣大學、中央警大、政治大學、清華大學 等大專院校

大綱

Agenda

01

網路攻擊鏈與資安事件回應

02

惡意程式攻防實務

03

社交工程攻防實務

04

數位鑑識概論

01
PART

網路攻擊鏈與資安事件回應

★ 資安攻擊的要件

★ 資安事件前中後作業項目

★ 資訊系統弱點

★ 網路攻擊鏈與資安事件回應

★ 資安法與資通安全事件通報

資安事件前中後作業項目

- 資安保險風險評估
  - ✓資安成熟度評估
  - ✓資安團隊
  - ✓資訊系統或資料鑑價
- 資安健診
  - ✓安全設定
  - ✓異常行為檢測
- 教育訓練

- 徹底根除避免再發
- 重新評估風險
- 教育訓練或模擬演練
- 實施改善並持續監控
- 敏感資料遮蔽並分享

惡意人員

事前防範

事件發生

事中應變

事後處置

- 攻擊向量分析
- 事件衝擊分析
- 各緊急事件編組協調分工
- 數位證據保全
- 有效遏制損失或阻止擴散
- 事件通報並追蹤管制

- 資安事件根因鑑定
- 法律訴訟支援
- 影響範圍清查
- 取得行為特徵

資安攻擊的要件

資安防禦

- ✓ 預防防禦
- ✓ 偵測告警
- ✓ 緊急應變
- ✓ 災害復原
- ✓ 數位鑑識

駭客

Motives(Goal)

Method

Vulnerability

動機(目的)：

為了展現技術能力或透過竊取資料或阻斷服務獲取金錢

方法：

透過的攻擊手法(破解密碼、社交工程、惡意程式.....)

脆弱點：

資訊可被利用的弱點或程式設計錯誤之處

資安事件特性

資安事件特性

反應時間短

- 攻擊時間不固定
- 攻擊通常會在短時間內完成

➢ 需要迅速有效的處理
➢ 需要定期檢查

種類複雜

- 可能蘊含多重攻擊
- 多為客製化惡意行為

➢ 需要準確判斷

不易保存數位證據

- 攻擊者會隱藏足跡
- 訴訟需要具備證據能力之數位證據

➢ 需要專業鑑識工具
➢ 需要符合國際標準數位鑑識程序

資安事件處理要點

降低衝擊

有效且即時的處理可以降低資安事件對資訊服務的衝擊，且可減少矯正預防的影響範圍

修補系統缺陷

可針對根因清查所有資訊主機，避免再次發生類似資安事件。並可用在訴訟、情資分享及教育訓練等用途

資通安全威脅與弱點

資訊安全框架

如ISO 27001、ITIL等等

資訊類

如：系統弱點、程式錯誤、未落實資安設定、新興資訊技術等等

實體環境

如天災、人員出入管制、電力供應、監控等等

人員類

如人性習慣、資安概念不足、技術傳承不完整、心生怨念等等

特殊活動

新系統或新服務上線、發表特殊言論、稽核、災害復原演練等等

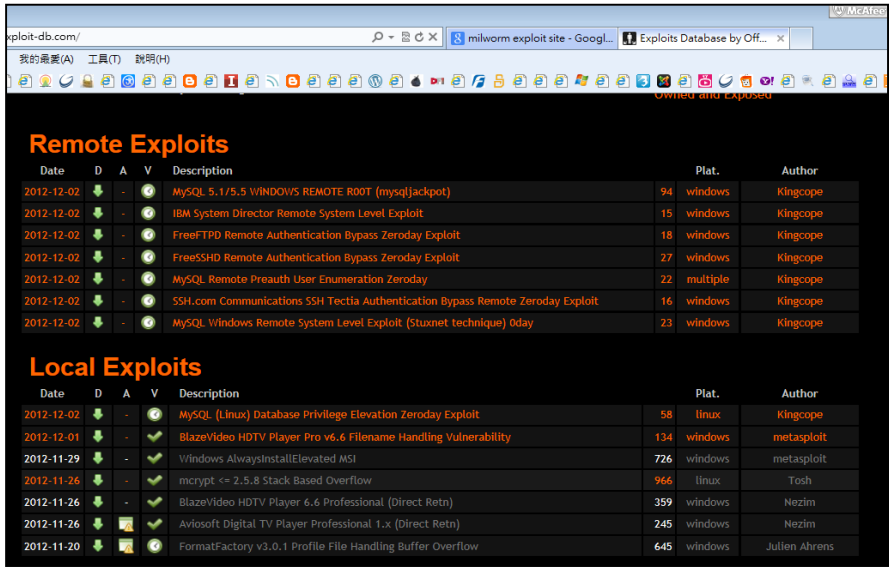
法規政策

如刑法民法、資通安全管理辦法、個人資料保護法等等

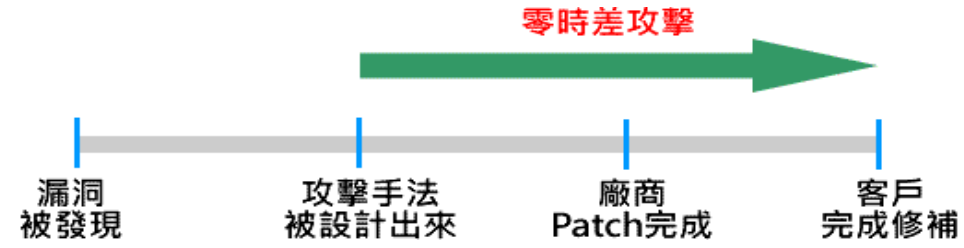
什麼是系統漏洞?

- 系統漏洞的攻擊方式是指利用電腦系統程式設計或維護時所留下的錯誤或後門程式(backdoor)進行侵入工作。

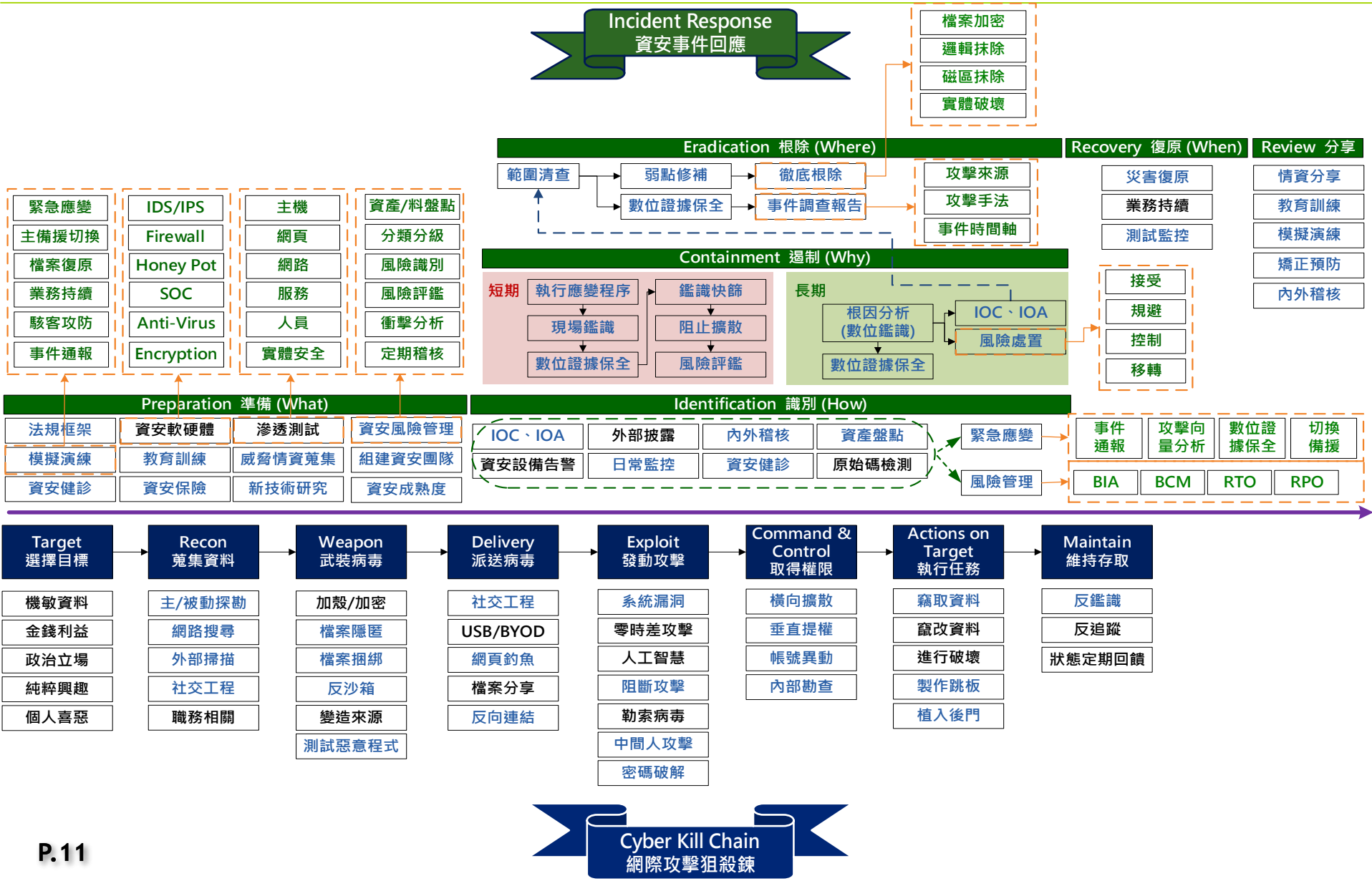
- 零時差(Zero-day)攻擊：事先取得軟體並破解其漏洞或缺陷，或在未有修補程式前，就被利用為攻擊標的



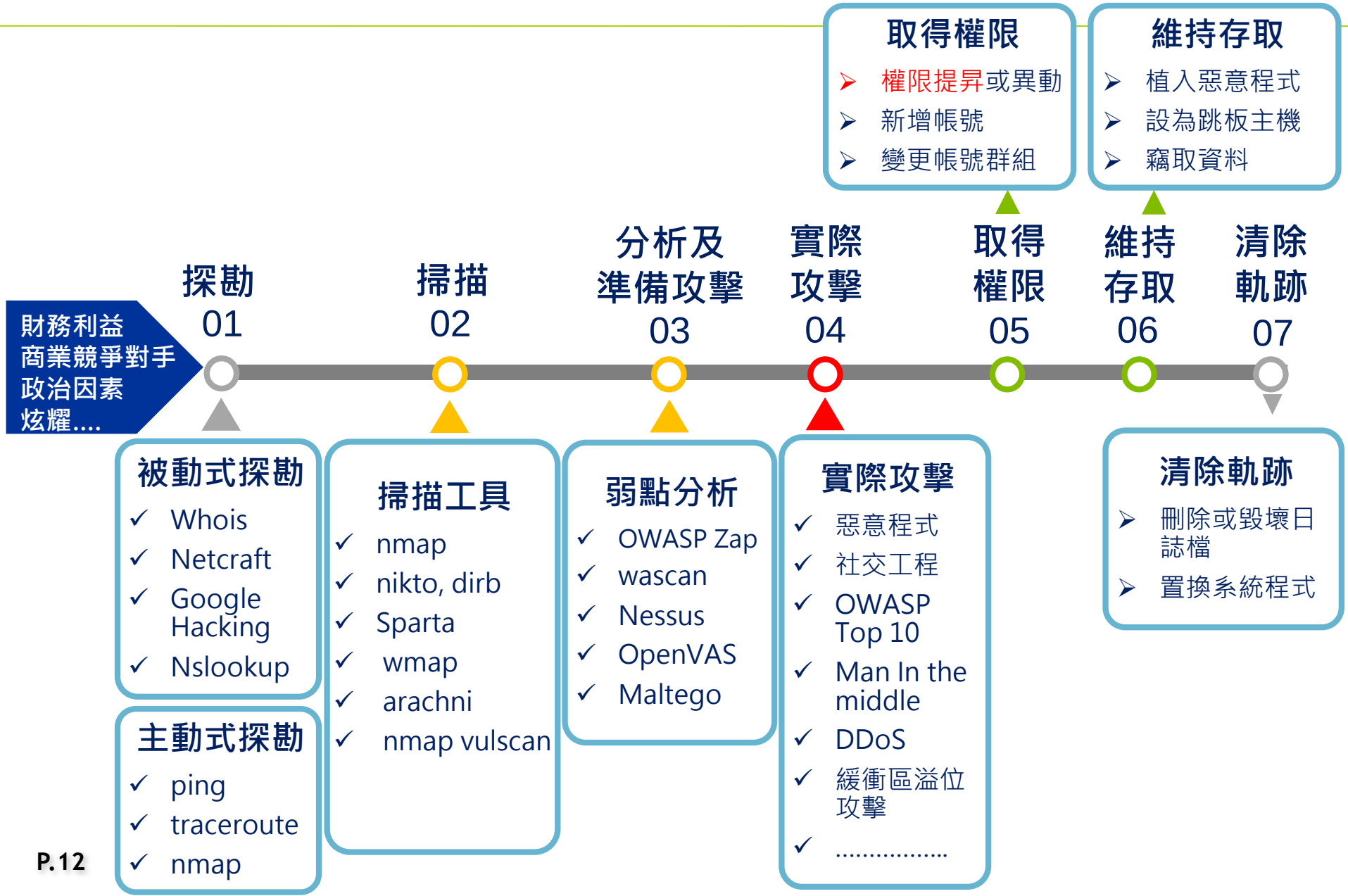

```
So here are the CVEs which Kurt meant to assign, but somehow
that mail never reached the lists.


* CVE-2012-5611 MySQL (Linux) Stack based buffer overrun PoC Zeroday
http://seclists.org/fulldisclosure/2012/Dec/4
https://bugzilla.redhat.com/show_bug.cgi?id=882599

* CVE-2012-5612 MySQL (Linux) Heap Based Overrun PoC Zeroday
http://seclists.org/fulldisclosure/2012/Dec/5
https://bugzilla.redhat.com/show_bug.cgi?id=882600

* CVE-2012-5613 MySQL (Linux) Database Privilege Elevation Zeroday
Exploit
http://seclists.org/fulldisclosure/2012/Dec/6
https://bugzilla.redhat.com/show_bug.cgi?id=882606

* CVE-2012-5614 MySQL Denial of Service Zeroday PoC
http://seclists.org/fulldisclosure/2012/Dec/7
https://bugzilla.redhat.com/show_bug.cgi?id=882607

* CVE-2012-5615 MySQL Remote Preauth User Enumeration Zeroday
http://seclists.org/fulldisclosure/2012/Dec/9
https://bugzilla.redhat.com/show_bug.cgi?id=882608
```



Cyber Kill Chain & Incident Response



駭客入侵程序


取得權限
權限提昇或異動
新增帳號
變更帳號群組
維持存取
植入惡意程式
設為跳板主機
竊取資料
財務利益
商業競爭對手
政治因素
炫耀....
探勘
01
掃描
02
分析及
準備攻擊
03
實際
攻擊
04
取得
權限
05
維持
存取
06
清除
軌跡
07
被動式探勘
Whois
Netcraft
Google Hacking
Nslookup
主動式探勘
ping
traceroute
nmap
掃描工具
nmap
nikto, dirb
Sparta
wmap
arachni
nmap vulscan
弱點分析
OWASP Zap
wascan
Nessus
OpenVAS
Maltego
實際攻擊
惡意程式
社交工程
OWASP Top 10
Man In the middle
DDoS
緩衝區溢位攻擊
.....
清除軌跡
刪除或毀壞日誌檔
置換系統程式

02
PART

惡意程式攻防實務

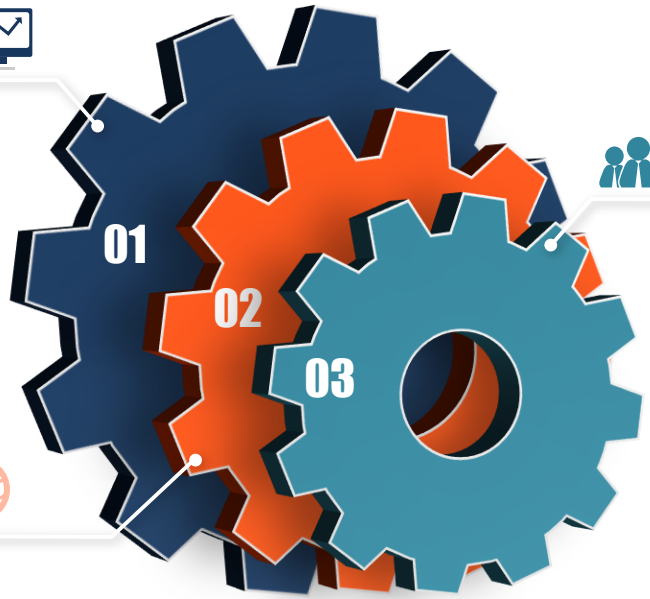
★ 惡意程式比較
★ 系統漏洞
★ 惡意程式攻防實戰

惡意軟體

- 可以是一段惡意程式碼或是一個惡意檔案，在未經使用者同意下，非法存取、變更、修改或刪除電腦系統的資料
- 以下是三種主要惡意軟體種類

病毒 (Virus)

- 可感染其他檔案
- 透過主動或被動傳播
- 感染主機數量隨時間而增加



蠕蟲 (Worm)

- 無法感染其他檔案
- 主動散佈自己
- 可以感染區域網路內具有相同弱點的主機

木馬(Trojan Horse)

- 無法感染其他檔案
- 只能被動散佈自己
- 一次只能感染一台主機

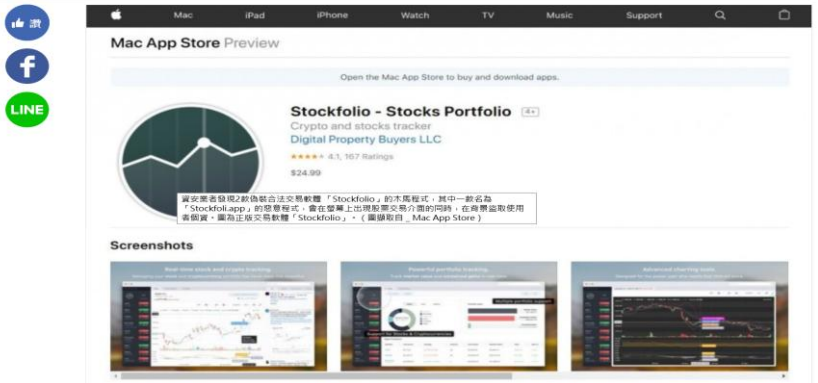
惡意程式相關新聞事件

自由時報 Liberty Times Net

即時 政治 社會 生活 國際 地方 人物 蒐奇 影音 財經 娛樂 寵伴 NEW
汽車 時尚 體育 3C 評論 玩咖 食譜 健康 地產 專區 TAIPEI TIMES

首頁 > 生活

Mac資安警戒！偽裝成股票交易軟體 惡意程式盜竊個資



資安業者發現2款偽裝合法交易軟體「Stockfolio」的木馬程式，其中一款名為「Stockfoli.app」的惡意程式，會在螢幕上出現股票交易介面的同時，在背景盜取使用者個資。圖為正版交易軟體「Stockfolio」。（圖擷取自_Mac App Store）

iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會 社群

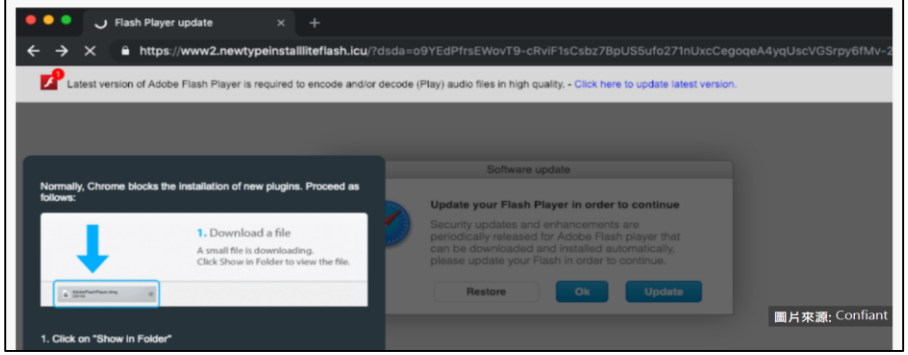
新聞

惡意程式藏身圖片，劫持500萬蘋果用戶流量

鎖定Mac及iOS用戶，駭客組織將惡意程式寫入圖片檔發動廣告攻擊，受影響網站單日損失超過120萬美元

文/ 林妍溱 | 2019-01-25 發表

讚 5.7萬 按讚加入iThome粉絲團 讚 552 分享



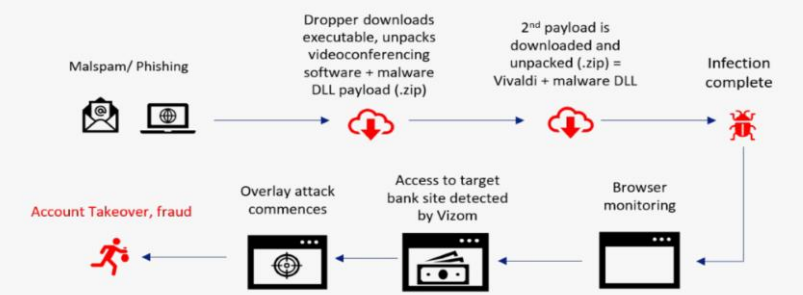
新聞

惡意程式冒充視訊軟體、瀏覽器為掩護，劫持網銀帳戶

惡意程式Vizcom發釣魚信誘騙受害者下載假造的視訊會議軟體，並以DLL劫持手法迴避Windows及端點防護產品偵測

文/ 林妍溱 | 2020-10-21 發表

讚 6.3萬 按讚加入iThome粉絲團 讚 139 分享



研究人員Chen Nahman指出，Vizcom使用現今愈來愈常見的DLL hijacking手法：當用戶啟動下載惡意DLL檔，會先以.zip檔型式進入AppData目錄，然後展開自動解壓縮，裏面包含了知名視訊軟體的binary及惡意DLL檔。這冒名DLL使Windows以子程序允許執行，同時以知名視訊軟體的身份潛藏在用戶電腦上，但是連向的是外部惡意伺服器。第二階段，Vizcom又以DLL劫持手法下載Chromium瀏覽器Vivaldi的binary及惡意DLL檔，然後在其掩護下開始攻擊行動。（圖片來源 / IBM）

美國公布搶劫全球銀行的北韓駭客集團BeagleBoyz分析報告

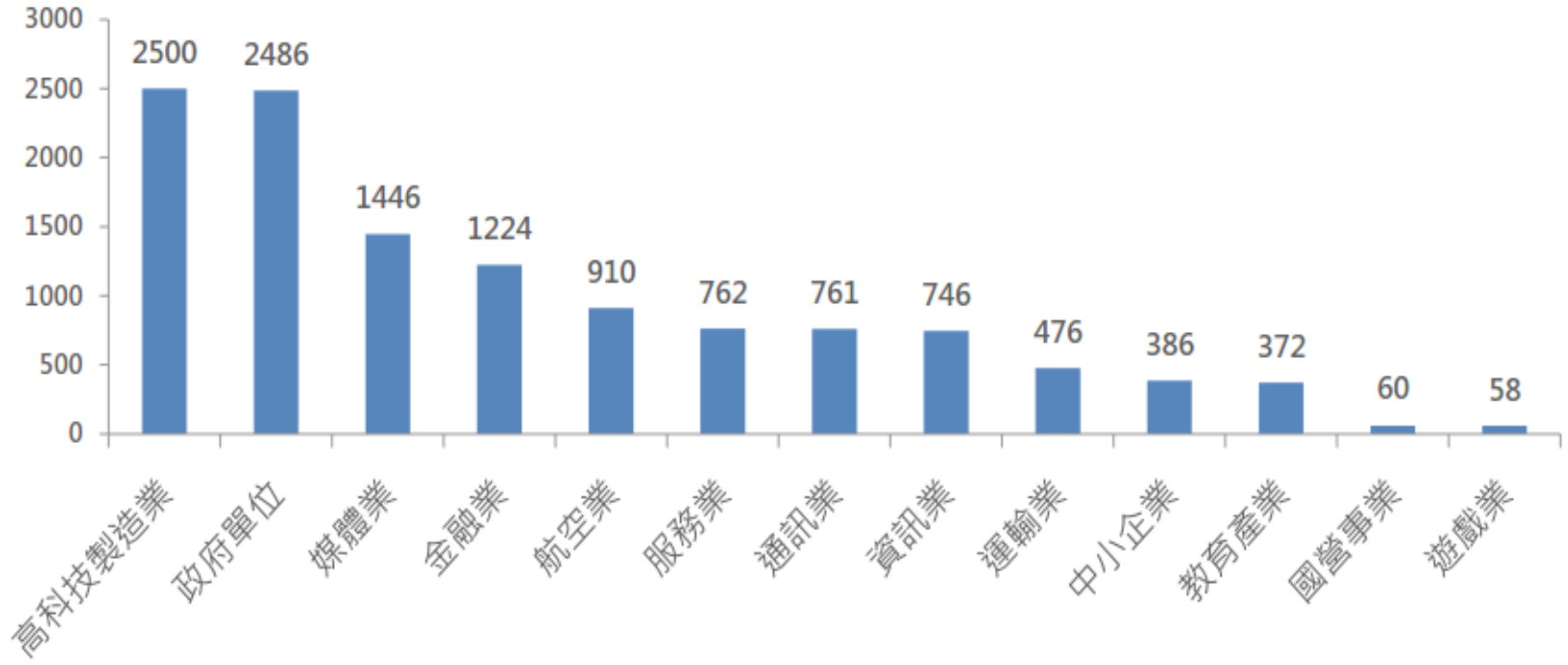
BeagleBoyz主要針對銀行與環球銀行金融電信協會（SWIFT）介接的終端系統，以及負責銀行支付交換應用的伺服器發動攻擊，曾成功自孟加拉銀行盜轉8千萬美元，讓散布在全球逾30個國家的ATM同時吐鈔

文/ 陳曉莉 | 2020-08-27 發表

讚 6.3萬 按讚加入iThome粉絲團 讚 99 分享

國內駭客入侵情形嚴重

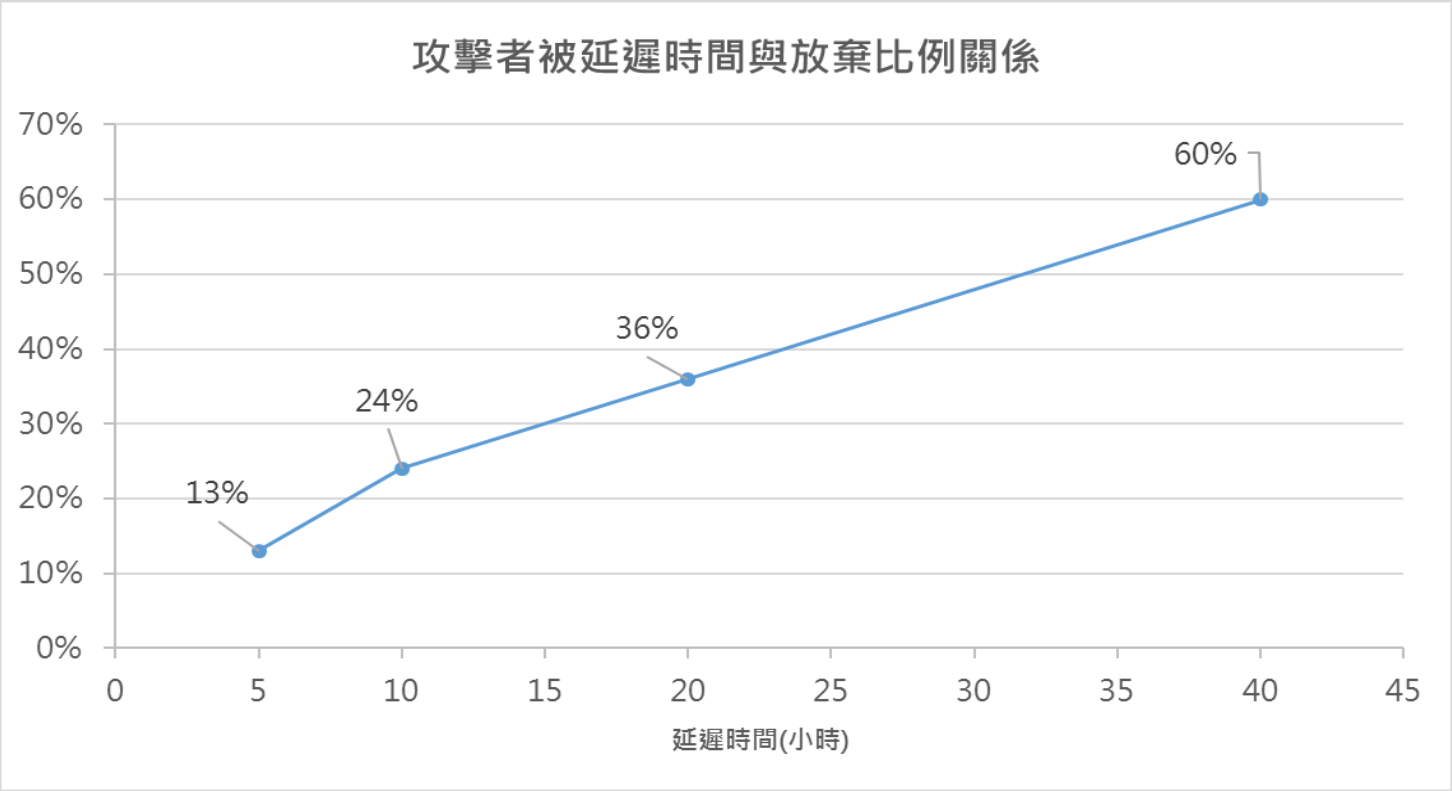
- 以政府單位為例，平均需要604天才能發現被駭客入侵
- 入侵來源99%為中國駭客
- 受侵害單位之中，有93.1%為高度受駭，即駭客完全掌握資訊系統，可任意活動。



資料來源：趨勢科技_資安威脅趨勢及駭客攻擊案例分享

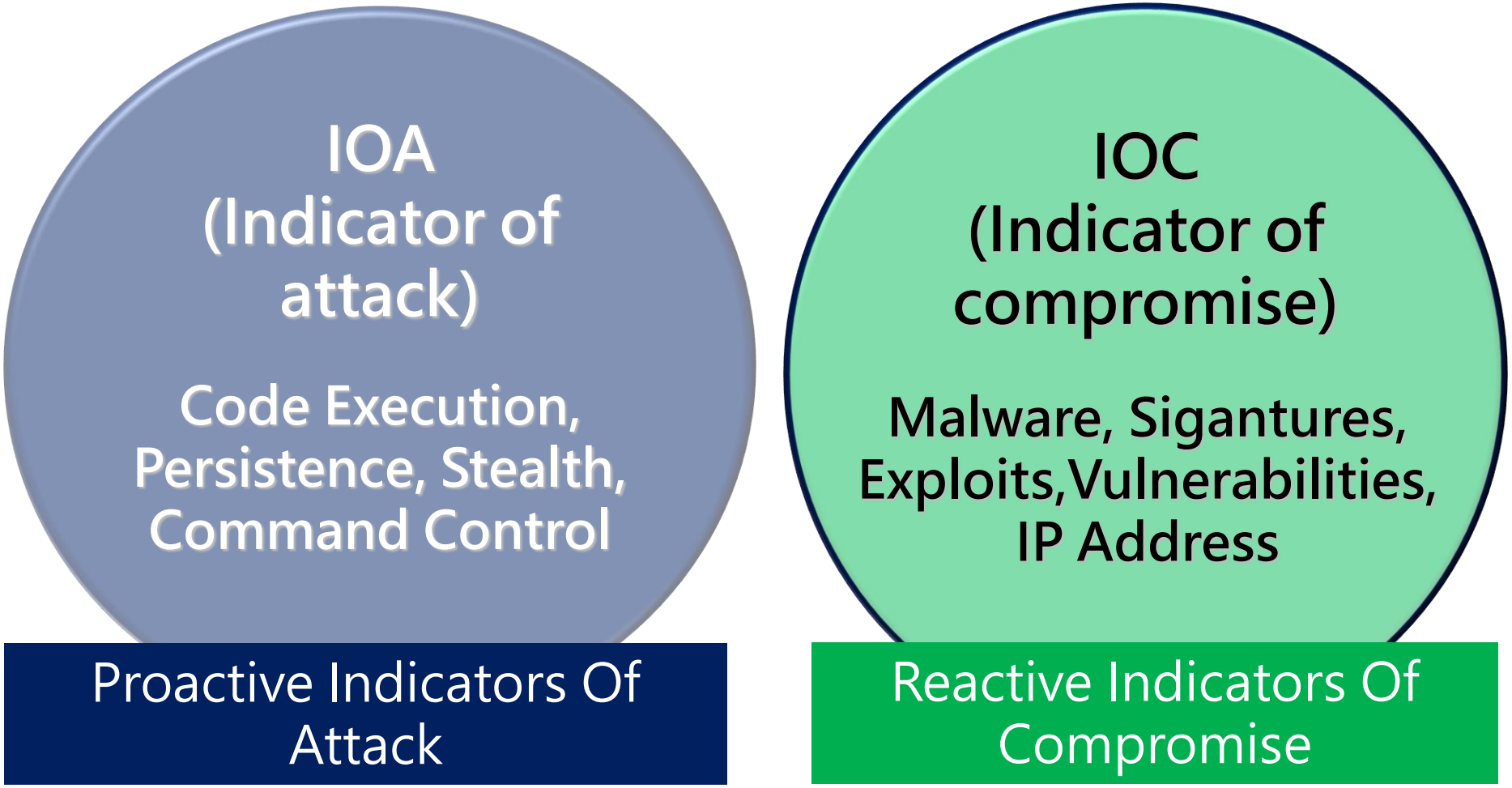
駭客入侵關鍵時刻

- 根據資安公司於2016.2.2發表之統計數據，攻擊者平均每年花費70小時攻擊傳統資安架構，若為更先進或優秀之資安架構則會花上147小時，且於209小時候完全放棄攻擊

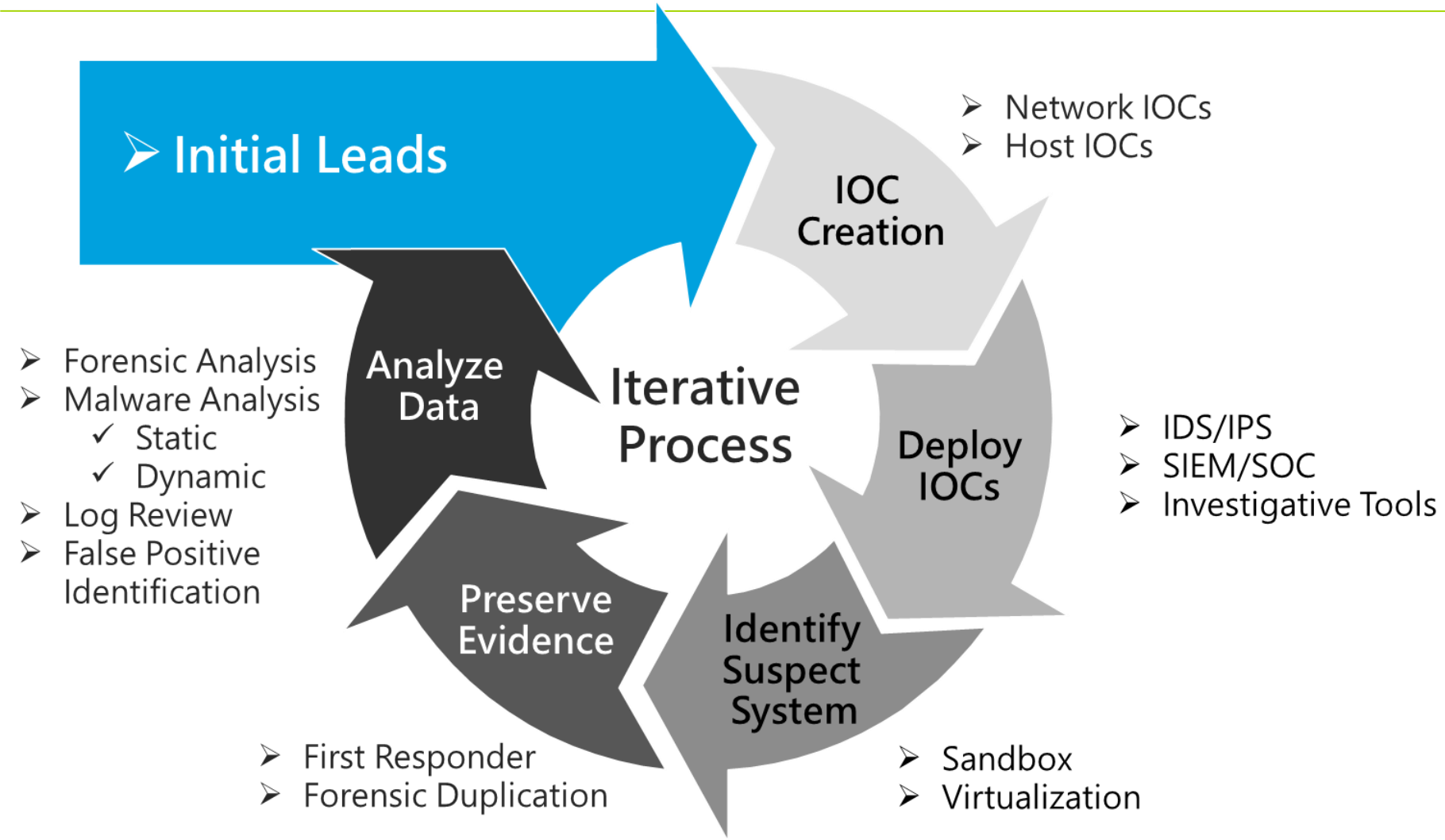


資料來源：http://www.csoonline.com/article/3028787/cyber-attacks-espionage/survey-average-successful-hack-nets-less-than-15-000.html

IOA 與 IOC

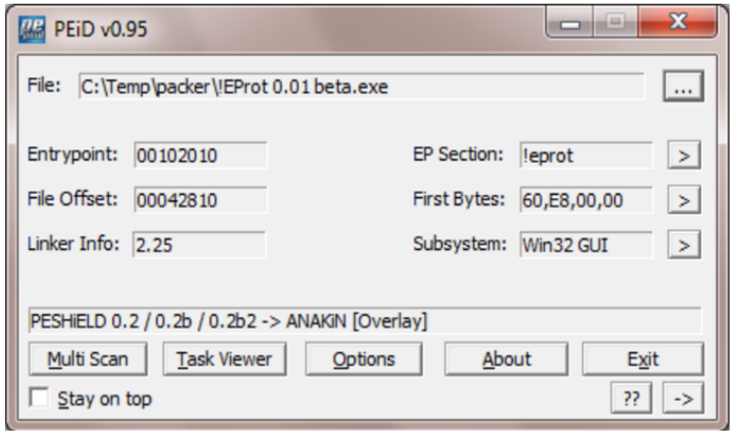

IOA
(Indicator of attack)
Code Execution, Persistence, Stealth, Command Control
IOC
(Indicator of compromise)
Malware, Sigantures, Exploits,Vulnerabilities, IP Address
Proactive Indicators Of Attack
Reactive Indicators Of Compromise

惡意程式分析生命週期


Initial Leads
IOC Creation
Network IOCs
Host IOCs
Deploy IOCs
IDS/IPS
SIEM/SOC
Investigative Tools
Identify Suspect System
Sandbox
Virtualization
Preserve Evidence
First Responder
Forensic Duplication
Analyze Data
Forensic Analysis
Malware Analysis
Static
Dynamic
Log Review
False Positive Identification
Iterative Process

靜態分析方式 (Static Malware Analysis)

- 靜態分析方式 (Static Malware Analysis)
  - 針對惡意程式樣本的程式碼與執行檔進行分析，找到符合特徵的部份並反解其功能
    - ✓ File Signatures
    - ✓ Strings within file
    - ✓ Portable Executable (PE) Headers + Resources



動態分析方式 (Dynamic Malware Analysis)

- 動態分析方式 (Dynamic Malware Analysis)
  - Monitoring Host Integrity：在動態分析開始前將欲進行分析的環境備份，以便在分析開始後對照惡意程式對系統做的行為
  - Observing Runtime Behavior：將惡意程式樣本置於環境中執行，觀察惡意程式感染宿主電腦後，電腦檔案系統的變化
  - 常見動態分析工具
    - Autoruns
    - cports-x64
    - Wireshark
    - Regshot
    - WhatChanged
    - Ollydbg

03
PART

社交工程攻防實務

★ 網路釣魚手法
★ 常見社交工程手法
★ 檔案變造

什麼是社交工程？

- 社交工程 (Social Engineering) 係利用人性弱點來進行詐騙，是一種非全面技術性的資訊安全攻擊方式，藉由人際關係的互動，來突破資通安全防護，遂行其非法的存取、破壞行為，以獲取帳號、通行碼、身分證號碼或其他機敏資料。

<來源:yahoo新聞 日期: 2019-07-16>
<來源:yahoo新聞 日期: 2019-11-01>
<來源:Ettoday 日期: 2019-11-11>

網路釣魚手法 – 假網頁假連結

iThome 新聞 產品&技術 專題 AI Cloud DevOps 資安 研討會 社群 科技防疫情報站 搜尋

新聞

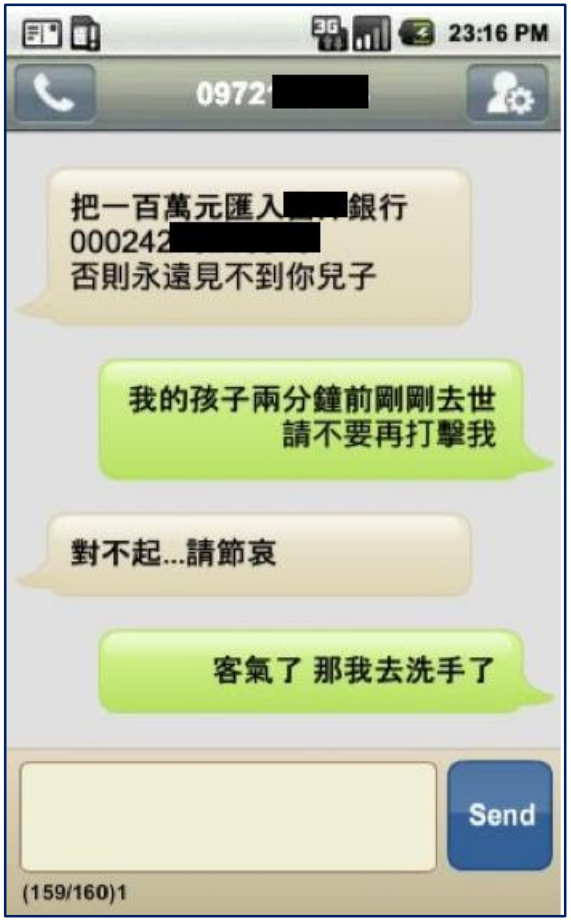
假冒銀行釣魚簡訊詐騙規模擴大，繼國泰世華、台新銀行後，中國信託今日也出現遭冒名的狀況，金融業者與民眾可千萬注意

近半個月來，假冒國內金融機關釣魚簡訊詐騙的狀況相當不尋常，不只出現假國泰世華、假台新銀行的釣魚簡訊，已造成30多位民眾上當受害，損失金額超過500萬元，今日（2月9日）再度出現假中國信託的釣魚簡訊。

文/ 羅正漢 | 2021-02-09 發表

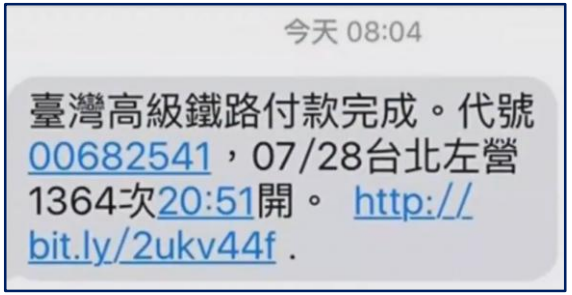
讚 6.6 萬 按讚加入iThome粉絲團 讚 4,510 分享

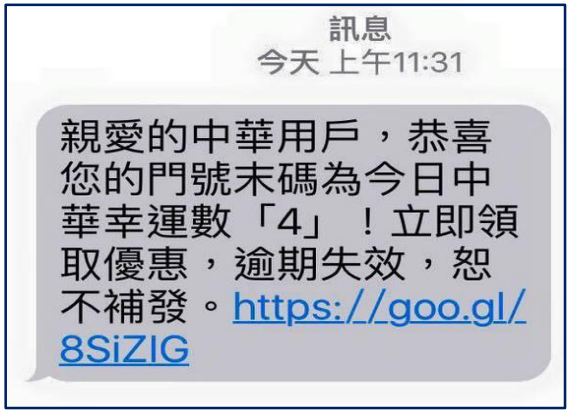
網路釣魚手法 – 假訊息


23:16 PM
0972[redacted]
把一百萬元匯入[redacted]銀行
000242[redacted]
否則永遠見不到你兒子
我的孩子兩分鐘前剛剛去世
請不要再打擊我
對不起...請節哀
客氣了 那我去洗手了
Send
(159/160)1


怎麼了嗎
我賴的資料不見了，需要好友輔助認證
是喔
所以給你手機號碼後呢?
?
0972-546299
幫我收封簡訊，收到簡訊驗證碼給我就好
傳給你了，有收到四位數的認證碼傳給我就好
我不會用耶~你打電話來教我好嗎?


訊息
+886[redacted]
編輯
通話
FaceTime
新增聯絡資訊
訊息
2014/6/15 下午5:02
您好,[新北市政府警察局]您涉嫌的案件處理結果通知單
http://goo.gl/u4drVi


今天 08:04
臺灣高級鐵路付款完成。代號00682541，07/28台北左營1364次20:51開。 http://bit.ly/2ukv44f .


訊息
今天 上午11:31
親愛的中華用戶，恭喜您的門號末碼為今日中華幸運數「4」！立即領取優惠，逾期失效，恕不補發。https://goo.gl/8SiZIG

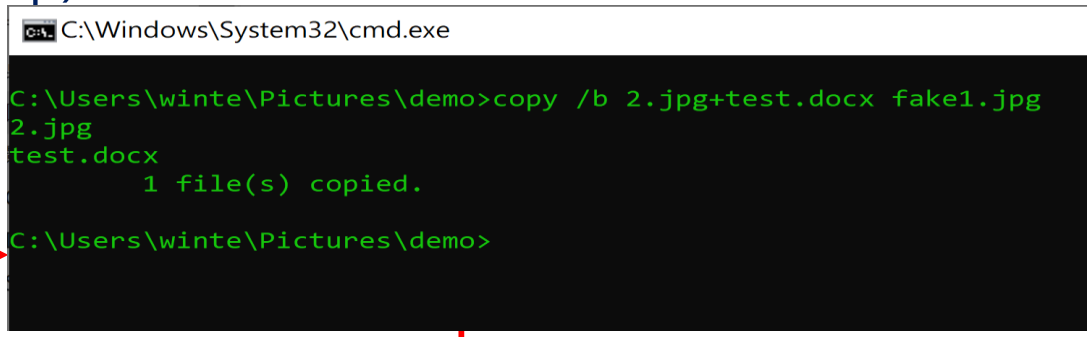
常見社交工程電子郵件主旨

- 駭客常會使用收信者有興趣的生活、政治、工作、情色等相關議題的主旨，提高被害者點擊惡意連結的意願

郵件種類	郵件標題
網路新知	太神奇！日本發明可觸摸3D影像
金融財經	銀行綜合對帳單 刷卡消費通知 水費電子通知單 您的App1e收據
八卦娛樂	iPhone 11間諜照曝光 愷樂遭父爆料！羅志祥來過我家好多遍
公務宣導	助妳好孕 - 打造友善生養城市 公教人員健檢辦法 Fw: 試算你家的二代健保費
廣告	部落格放廣告 做公益也貼補家用 iPhoneXS 0元手機帶回家
新聞時事	子彈穿腦 男「哈啾」噴出 311地震最新資訊及捐款帳號
旅遊休閒	東京天空樹長高 目標世界NO1 FW：探索台灣「月世界」景點 香港迪士尼 兩天萬元有找

社交工程 - 檔案變造

- 偽造連結或可能含有惡意程式的附件
  - 含有執行檔(EXE)
  - 含有惡意程式的影片檔(wmv)
  - 含有惡意程式的Office文件(doc)
  - 含有惡意程式的圖檔(jpg)
  - 含有惡意程式的壓縮檔(zip)



電子郵件隱藏病毒範例

+Tso 搜尋 圖片 地圖 Play YouTube 新聞 Gmail 雲端硬碟 日曆 更多

Google

新功能！我們已在 Google Play 和 Apple App Store 上推出更新版的 Gmail 行動應用程式。 關閉

Gmail 更多

撰寫

收件匣 (10,679)

寄件備份

草稿 (11)

社交圈

[Imap]/Sent

[Imap]/Trash (69)

更多

Fwd: 同學聚會事 收件匣 ×

[redacted] Chen <sc[redacted]@gmail.com>

寄給 [redacted]

Dear 瑞[redacted]

原定週末（12月09日）的國中同學聚會活動正常舉行！
目前已有5位女生確認赴約了喔~ (^_^)

集合時間地點不變，上午11:00武陵農場門口。

此次活動有不同於以往的安排，有驚喜等待著大家!

活動安排見附檔，密碼8888，有疑問敬請致電。

時祺

陳[redacted] CHEN)
Department of Energy
Mitsui & Co. (Taiwan) Ltd.
Tel: (04)2[redacted]

1209聚會安排.doc
131K 檢視 下載

04
PART

數位鑑識概論

★ 數位鑑識定義

★ 數位鑑識種類

★ 數位鑑識工具

★ 數位鑑識國際標準程序

數位鑑識(Digital Forensic)定義

定義 Definition

- ✓ 「The application of forensic science technique to computer-base material.」即應用嚴謹的程序及科技的方法去處理數位資訊設備相關鑑識工作
- ✓ 在法令規範下，利用科學驗證的方式來調查數位證據：針對數位證據的還原、擷取、分析的過程，還原事件原貌，以認定事實之數位資料，可作為法庭訟訴之依據

目的 Purpose

- ✓ 辨視肇事原因與人員以區分責任
- ✓ 為未來或事後法律行動保留證據
  - ✓ 民事案件：可與專業數位鑑識公司聯繫，或於組織內部制定可遵循且嚴謹的鑑識流程
  - ✓ 刑事案件：可向執法機關通報處理

數位鑑識國內外實際案例

媳婦「謊騙歹徒綁架」佈局殺婆婆？ 證詞遭Apple Watch戳破

▲Apple Watch成了破案關鍵。圖為示意圖。（圖／記者洪聖壹攝）

國際中心／綜合報導

澳洲阿得雷德曾於2016年9月發生一起命案，57歲的婆婆尼爾森（Myrna Nilsson）當時在自家洗衣間遇害，她26歲的媳婦卡洛琳（Caroline Nilsson）事後聲稱她與婆婆都遭到陌生男子的綁架與襲擊。然而，檢方最近分析尼爾森手上的Apple Watch認為，卡洛琳的說法有矛盾之處，她將於6月再次開庭。

自由時報 Liberty Times Net

即時 熱門 政治 社會 生活 國際 地方 蒐奇 影音 財經 娛樂 寵伴 汽車
時尚 體育 3C 評論 玩咖 食譜 健康 地產 專區 TAIPEI TIMES 求職

首頁 > 國際

誤認74年！歷史學家研究發現「硫磺島升旗」士兵另有其人

6名美國海軍陸戰隊隊員在硫磺島摺鉢山豎立美國國旗，成為最經典的歷史照片之一，不過其中1名升旗手身分在這70餘年來都被誤認了。（圖擷自Wiki）

2019-10-17 16:10:59

〔即時新聞／綜合報導〕1945年2月23日正在激戰中的硫磺島，6名美國海軍陸戰隊隊員在摺鉢山豎立美國國旗，在第二次立旗時被隨軍記者拍下，成為歷史最經典的照片之一，升旗手也成為軍券購買的宣傳，但在經過各方面研究後，發現其中一名升旗手身分在這70餘年來都被誤認了。

歷史學者分析發現旗手另有其人

綜合美國媒體報導，長期研究硫磺島戰役的3名軍事歷史學家佛利（Stephen Foley）、斯彭斯

自由時報 Liberty Times Net

即時 熱門 政治 社會 生活 國際 地方 蒐奇 影音 財經 娛樂 寵伴 汽車
時尚 體育 3C 評論 玩咖 食譜 健康 地產 專區 TAIPEI TIMES 求職

首頁 > 社會

至少30人受害！廁所通便器放針孔偷拍 警逮「攝狼」工程師

警方查扣邱嫌偷拍器具。（記者王冠仁翻攝）

2019-05-05 20:47:11

首次上稿 09:59

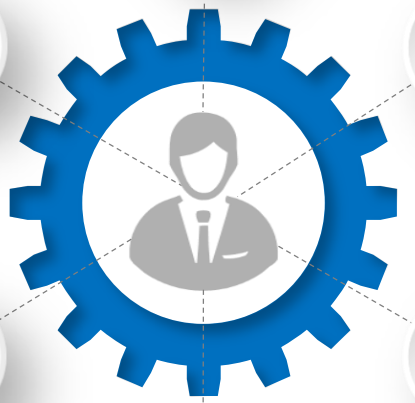
更新時間 20:47

〔記者王冠仁／台北報導〕台北市中正區一家超商的廁所內，之前被民眾發現有偷拍狼在通便器上安裝針孔攝影機，警方檢視偷拍檔案，發現有30多名民眾遭偷拍。警方調閱監器畫面追查，鎖定47歲邱

數位鑑識種類


Fraud Forensics
Network Forensics
Multimedia Forensics
Cloud Forensics
Storage Forensics
Mobile Forensics
Computer Forensics
IoT Forensics
Malware Forensics
Database Forensics
Crime Digital Investigation Intelligence
Recuva
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
cellebrite

鑑識分析人才核心能力



1 資訊安全基本認知

網路攻擊方式、資訊安全事件回應等
數位鑑識基本觀念

2 資訊法律認知

資訊倫理議題
網路犯罪、個資保護、著作權

3 電腦鑑識國際標準

ISO27037、 ACPO、NIJ
現場鑑識流程

4 現場鑑識

現場鑑識工具操作
現場鑑識工具功能限制與比較

5 數位鑑識工具操作

EnCase、Open Source
網路封包鑑識
行動裝置鑑識
揮發性資料鑑識
惡意程式鑑識

6 鑑識案件分析實務

數位鑑識案件分析方法
Windows、Linux系統分析實務
反鑑識手法剖析

數位鑑識工具


EnCase Portable
Triage G2
Tableau
F-Response
現場鑑識工具
TX1
Falcon
TD3
Dossier
數位證據複本工具
Intella
i2
VFC2
Passware
其他鑑識工具
EnCase
Magnet AXIOM
FTK
鑑識調查分析工具
鑑識工具
Log Reviewer
Message Analyzer
ELK
日誌及圖像鑑識工具
Adroit Photo Forensics
SANS-SIFT
Antopsy
記憶體鑑識工具
Volatility
Bulk Extractor
EnCase Imager
FTK Imager
網路鑑識工具
NetworkMiner
WireShark
Kali Linux
Caine
手機鑑識工具
Cellebrite
XRY
Oxygen
Blackbag

數位證據來源

網路或應用程式

- ✓瀏覽器紀錄
- ✓應用程式紀錄

系統限制

- ✓防火牆規則
- ✓帳號權限及列表
- ✓存取控制規則

作業系統

- ✓系統暫存檔
- ✓執行紀錄或日誌
- ✓系統Metadata

未分配或未使用空間

- ✓未分配(Unallocated)空間：磁區中刪除資料
- ✓未使用(Unused)空間：刪除或調整磁區

儲存媒體

- ✓電腦硬碟、記憶卡
- ✓網路儲存設備
- ✓記憶體或暫存空間

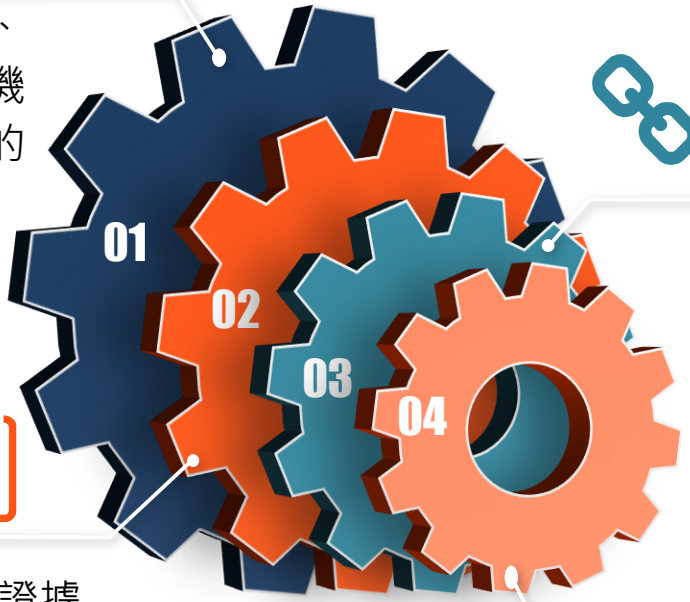
實體設備

- ✓電腦/伺服器/筆記型電腦
- ✓行動影音設備
- ✓網路設備

數位證據處理準則

記錄所有的動作

- 靜態資訊可用相機、連續動作可用攝影機
- 蒐證現場環境及標的主機皆為記錄範圍



確認證據副本與原始證據之關聯

- 須證明副本與原始證物相同
- 須說明證據檔案出處
- 須將證據檔案與特定帳號或對象連結

確保數位證據符合三大原則

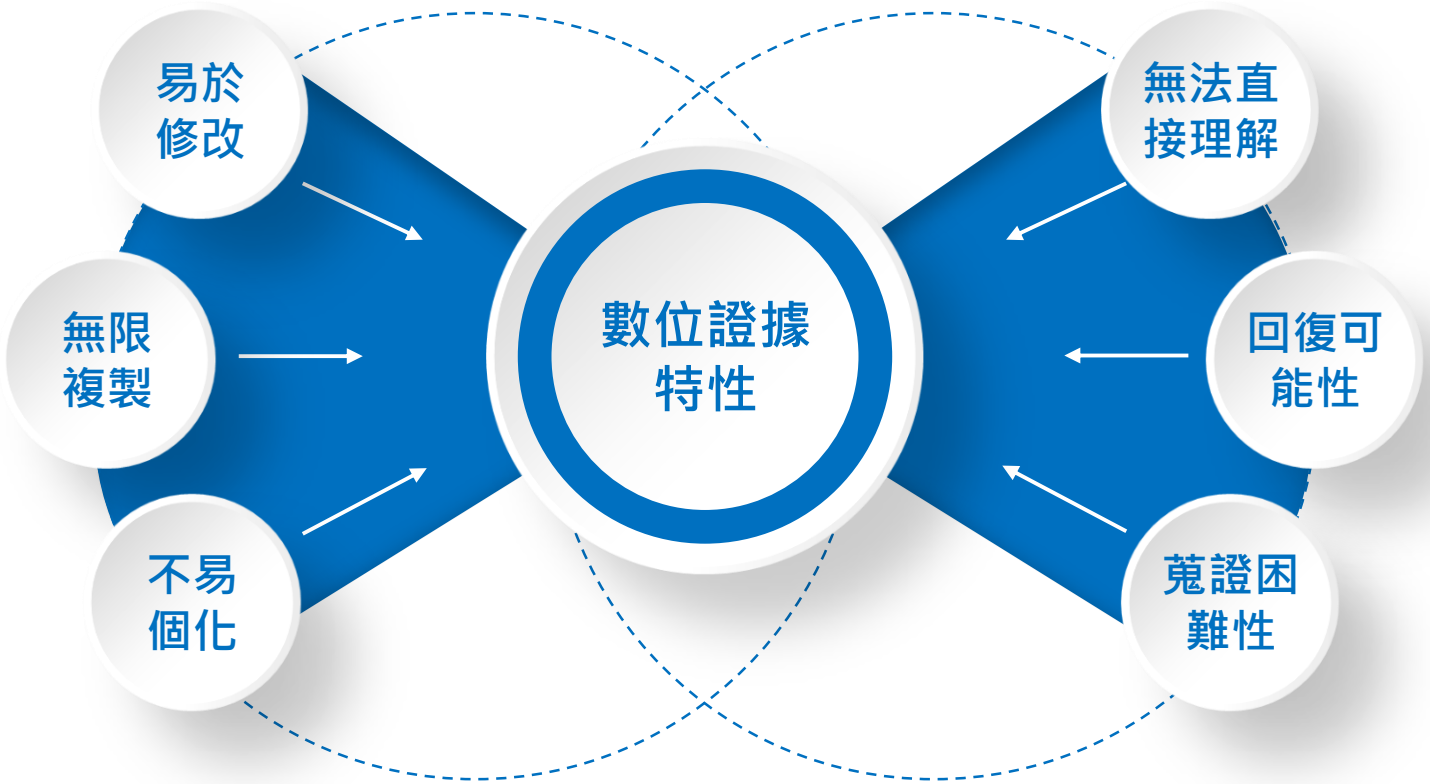
- 相關性：應能證明所取得證據與調查目標有關
- 可靠性：所有處理過程應該符合可驗證與可重複性
- 充分性：蒐集到足夠證據進行適當的調查

確保數位證據有效

- 避免數位證據被污染
- 確保證據監管鏈完整且正確

數位證據之定義與特性

- 數位證據（Digital Evidence）
  - 數位證據扮演輔助性的角色，用來加強證明事實，數位證據不能作為唯一之絕對證據，仍須環境證據佐證其證據證明力



數位鑑識作業階段

現場蒐證(Identify , Collect)

1. 辨識數位證物
2. 防止數位證據被污染
3. 需完整取得數位證據並執行驗證

證據封存及運送(Preserve)

1. 防止數位證物遭到破壞
2. 確保證據監管鏈不中斷

鑑識分析(Analysis)

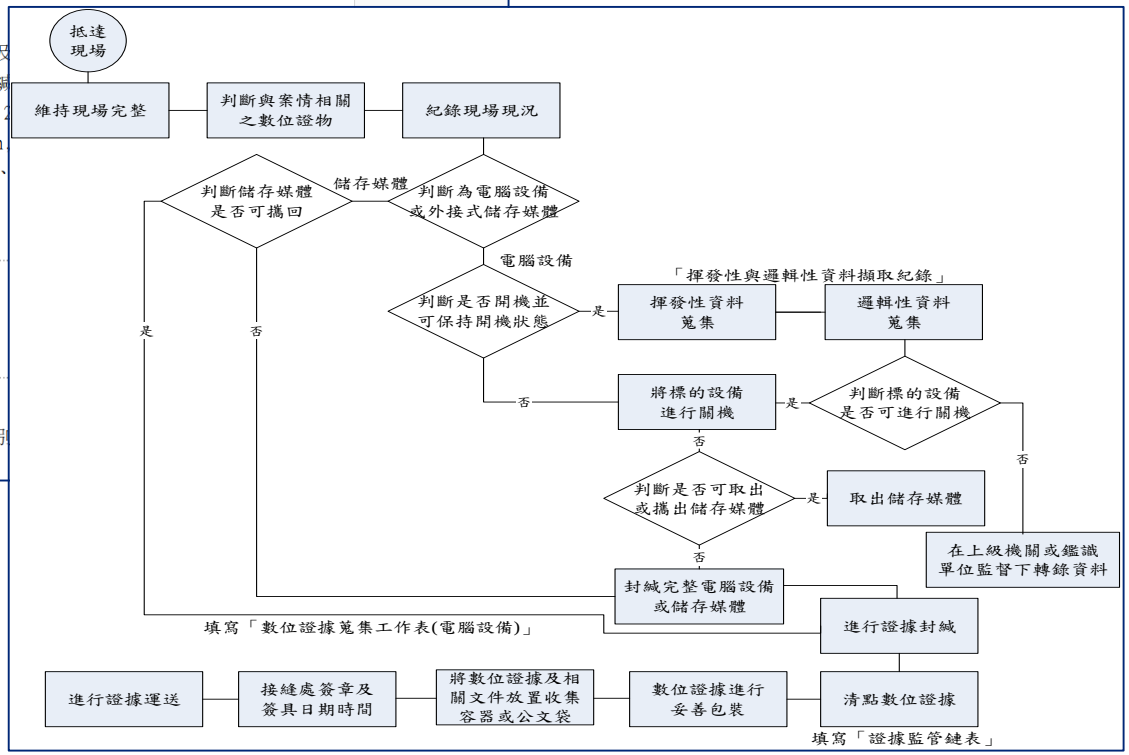
1. 分析攻擊或資安事件來源
2. 還原攻擊或案件原貌
3. 列出案件相關時間軸

報告及法院呈現(Present)

1. 僅呈現與本案相關證據
2. 舉證之所在，敗訴之所在

數位鑑識作業階段(續)


目前線上： 630 人，瀏覽人次：380831523
會員登入 | 加入會員
植根法律網
www.rootlaw.com.tw
回到首頁
植根書城
法律專欄
手機版本
法規檢索
令函判解
英譯法規
裁 判 書
書狀例稿
契約範本
植根服務
相關網站
法規資訊
法規名稱： 政府機關（構）資安事件數位證據保全標準作業程序
時間： 中華民國104年8月4日
所有條文
條文檢索
歷史沿革
相關令函
相關判解
制定依據
附屬法規
所有條文
友善列印
回上一頁
一、訂定目的
為使各級政府機關（構）於執行資安事件調查時能有效保全及
位證據，及執行人員於執行數位證據識別、蒐集、擷取、封
作業時有所依循，爰參考相關數位鑑識國際標準（ISO／IEC
uidelines for Identification, Collection, Acquisition
reservation of Digital Evidence ，數位證據識別、蒐集、
保存指引），特訂定本作業程序。
二、適用機關
各級政府機關（構）（以下簡稱各機關）。
三、適用時機
各機關基於資安事件之調查，需進行電腦系統之數位證據識別
、擷取、封緘及運送作業時，適用本作業程序。


抵達現場
維持現場完整
判斷與案情相關之數位證物
紀錄現場現況
判斷儲存媒體是否可攜回
儲存媒體
判斷為電腦設備或外接式儲存媒體
電腦設備
判斷是否開機並可保持開機狀態
「揮發性與邏輯性資料擷取紀錄」
揮發性資料蒐集
邏輯性資料蒐集
將標的設備進行關機
判斷標的設備是否可進行關機
判斷是否可取出或攜出儲存媒體
取出儲存媒體
在上級機關或鑑識單位監督下轉錄資料
封緘完整電腦設備或儲存媒體
填寫「數位證據蒐集工作表(電腦設備)」
進行證據封緘
進行證據運送
接縫處簽章及簽具日期時間
將數位證據及相關文件放置收集容器或公文袋
數位證據進行妥善包裝
清點數位證據
填寫「證據監管鏈表」
是
否

資訊安全實用觀念

- ✓ 沒有百分之百的資訊安全，得靠每個人從小地方一起努力！
- ✓ 所有的個人資訊設備都不是為了資訊安全設計的
- ✓ 駭客攻擊....從早到晚
- ✓ 讓自己麻煩就是讓駭客麻煩

資料銷毀或加密防護

Q: 要如何才能完整銷毀儲存媒體?

Thank You!