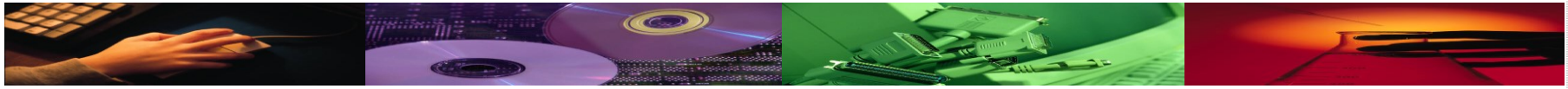
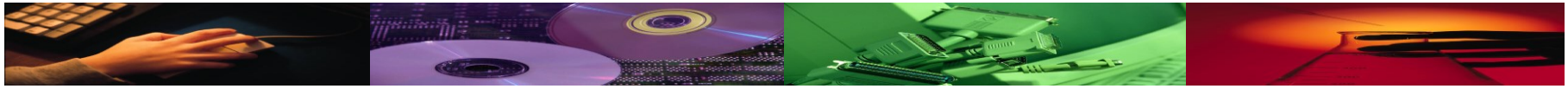


資安威脅的潛在危機與防範

112年11月14日

講師：NII 產業發展協進會 王俊凱 執行長

課程大綱



資安的威脅與新知

資安威脅現況

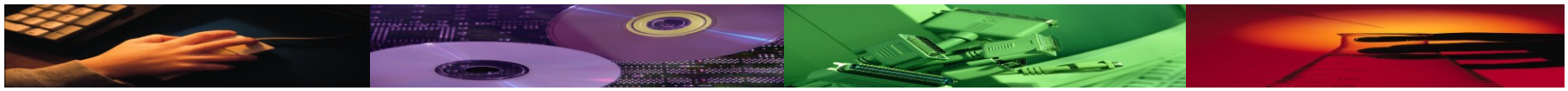
資安威脅趨勢

我們與駭客的距離

認識資安問題

建立應對技能

課程大綱

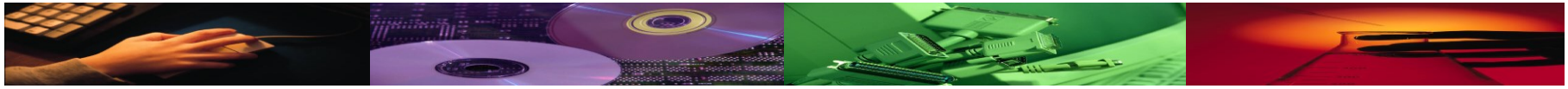


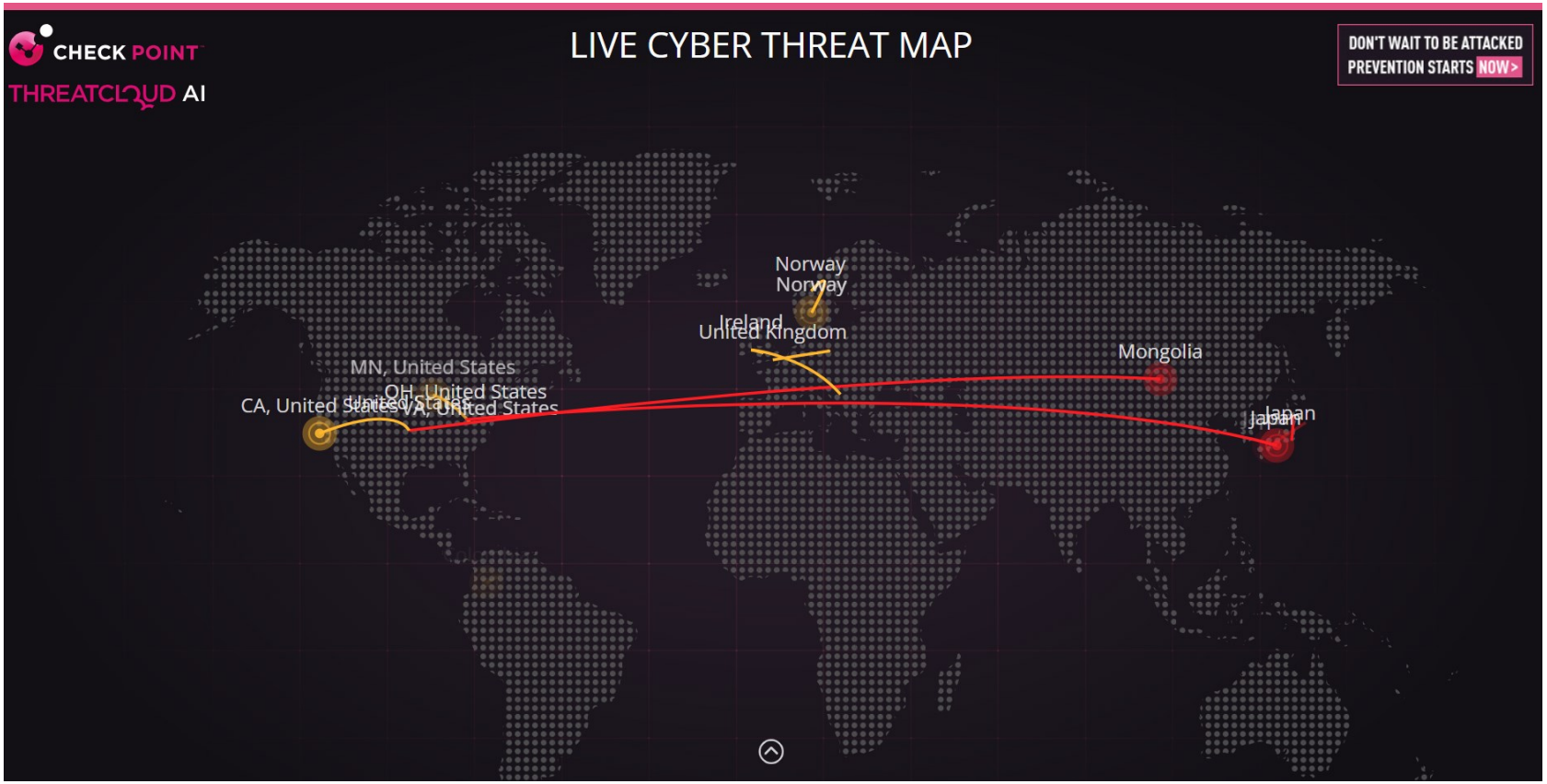
資安的威脅與新知

資安威脅現況

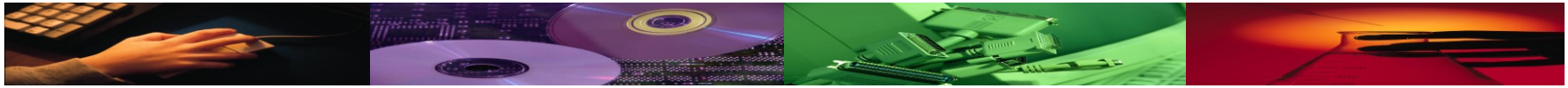
資安威脅趨勢

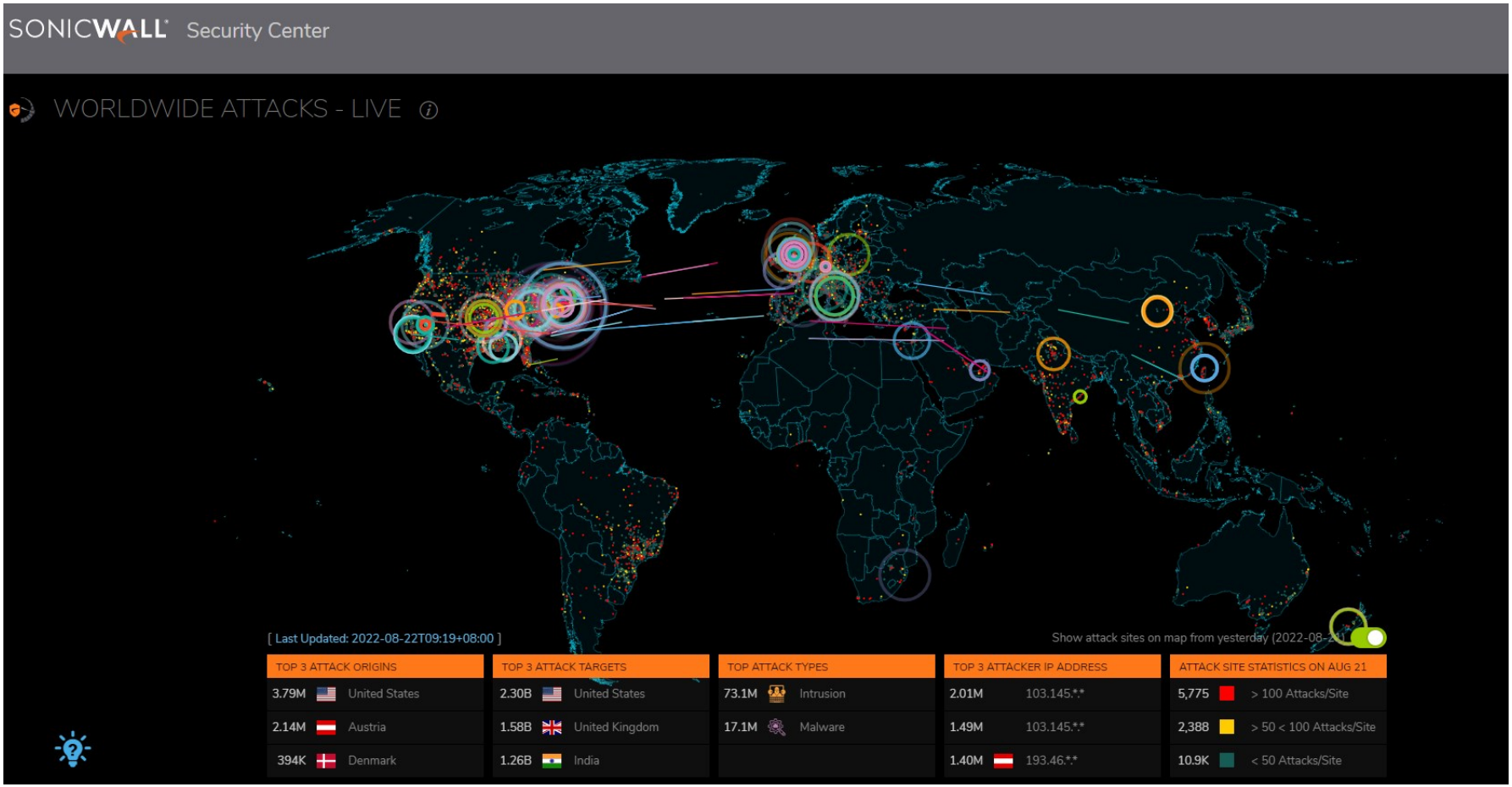
資安威脅現況(1)



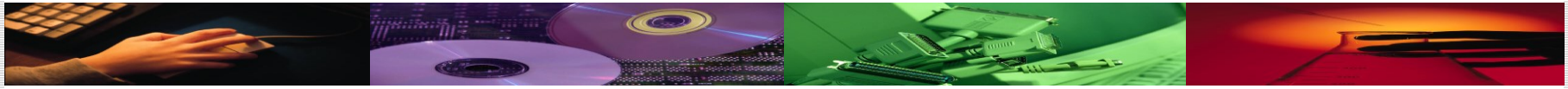


資安威脅現況(2)



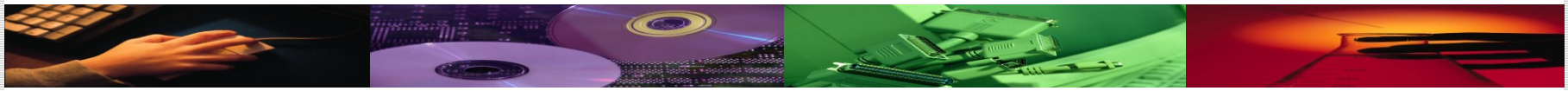


2022年國內上市櫃公司資安重大事件-1



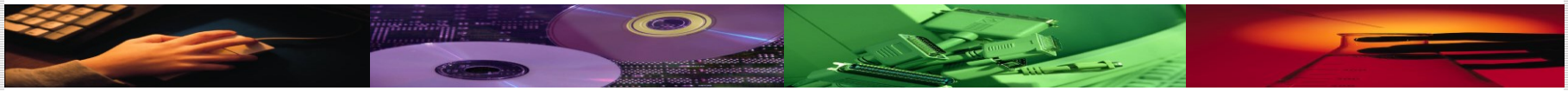
日期	公告公司	公告標題
2022.12.16	亞通	說明本公司遭受駭客網路攻擊事件
2022.12.01	麗臺	本公司遭駭客網路攻擊
2022.11.29	雄獅	說明本公司遭受駭客網路攻擊事件
2022.11.04	統領	說明部份資訊系統遭受駭客網路攻擊
2022.10.17	大拓-KY	說明子公司日本大拓資訊系統遭受病毒攻擊

2022年國內上市櫃公司資安重大事件-2



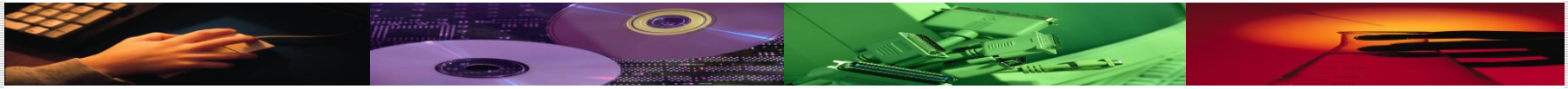
日期	公告公司	公告標題
2022.09.20	金橋	說明本公司遭病毒感染
2022.09.08	淳紳	**公告本公司部份資通系統遭病毒攻擊**
2022.07.22	台灣虎航	說明本公司遭受駭客網路攻擊事件
2022.07.18	永昕	說明部份資通系統遭病毒攻擊
2022.03.16	健鼎	本公司部份資訊系統遭受駭客網路攻擊事件說明
2022.01.22	台達電	說明部份資訊系統遭受駭客網路攻擊

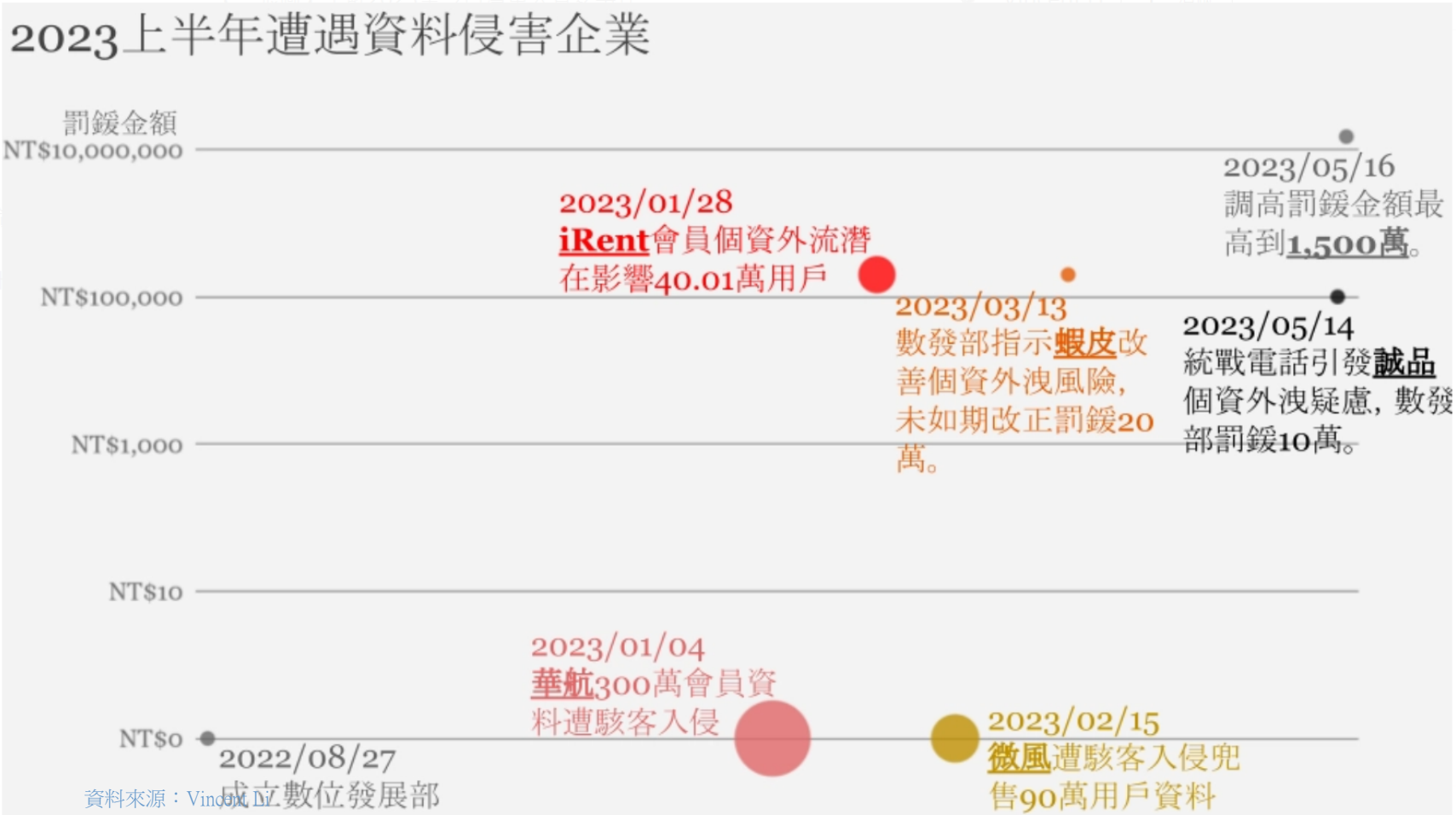
2023上半年國內上市櫃公司資安重大事件



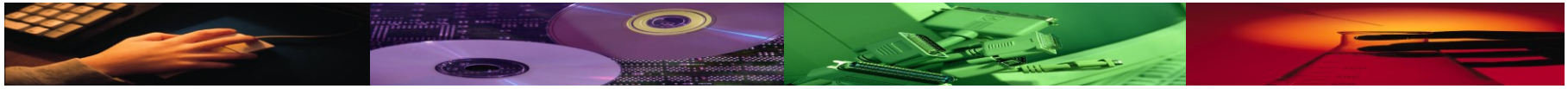
日期	公告公司	公告標題
2023.06.19	環天科	本公司部分資訊系統遭受駭客網路攻擊
2023.05.30	正新	代子公司Cheng Shin Rubber USA, Inc 公告部份資訊系統遭受駭客網路攻擊事件說明
2023.05.14	誠品生活	說明經濟日報112年5月14日14時10分網路新聞即時報導：誠品疑出現個資外洩，數位部要求完整說明…
2023.04.14	金鼎科	說明本公司部分資料遭受駭客網路攻擊事件
2023.04.07	微星	本公司部分資訊系統遭受駭客網路攻擊
2023.03.28	立德	立德電子部份資訊系統及備份系統遭受網路攻擊事件說明
2023.03.14	鋼聯	代子公司台鋼資源股份有限公司公告說明部份資訊系統遭受駭客網路攻擊
2023.03.06	宏致	本公司部份資訊系統遭受駭客網路攻擊事件說明
2022.02.12	華航	華航已全面加強資安系統防堵 配合警方偵辦個資事件

2023資料遭侵害的企業(上半年)





資訊安全威脅趨勢



1. 供應鏈攻擊

2. 資料安全威脅

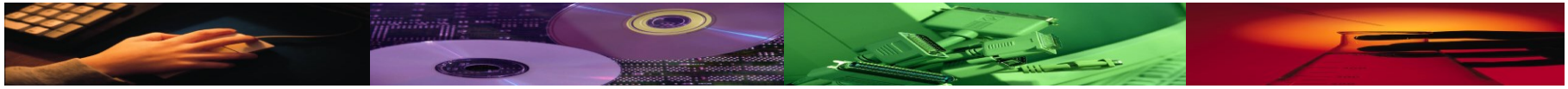
3. 雲端環境威脅

4. 勒索軟體攻擊

5. 漏洞利用攻擊

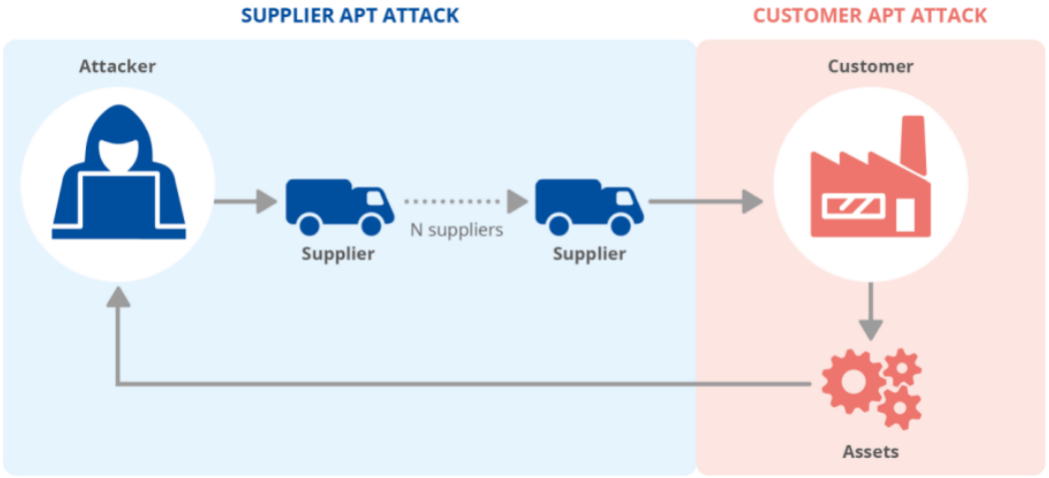
6. 挖礦劫持攻擊

供應鏈攻擊(1)

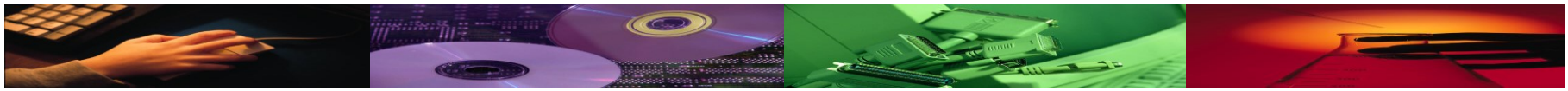


摘要說明

- 因為組織實施更強大的安全防護，攻擊者只好退而其次轉向服務供應商
- 一旦攻擊成功就可以影響使用該供應商的所有客戶
- 透過系統下線、經濟損失或聲譽受損等方式來產生重大影響

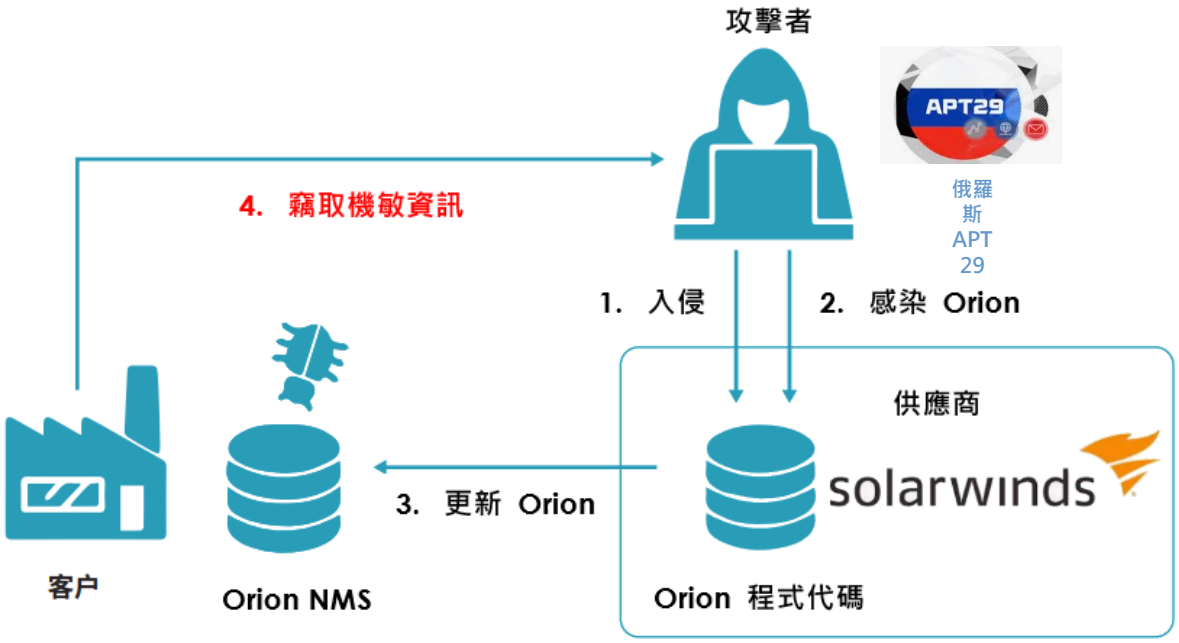


供應鏈攻擊(2)

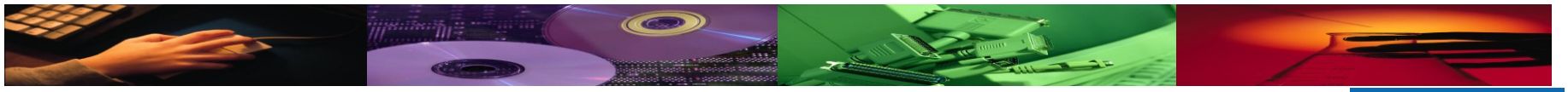


知名的供應鏈攻擊事件 (Dec-2020)

- Solarwinds : IT 管理、遠端監控軟體公司
  - 竊取客戶機敏資訊
    - 美國國防部、國務院、國土安全部...聯邦機構

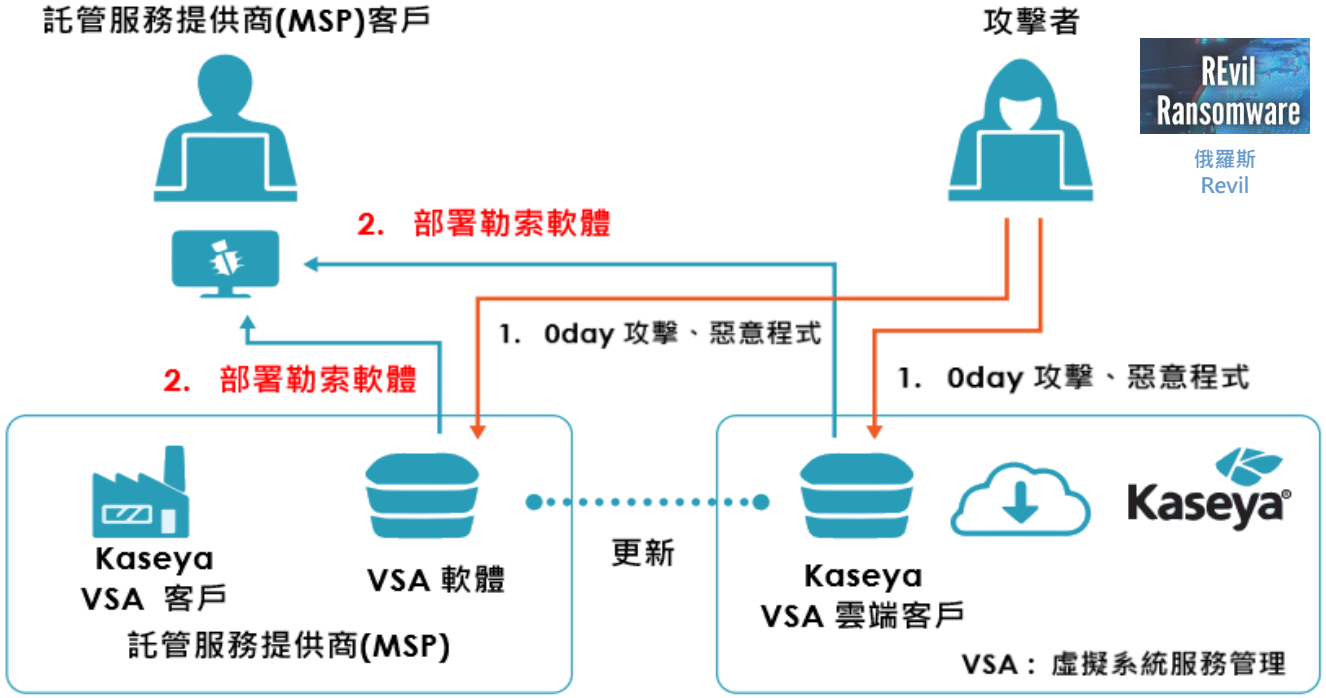


供應鏈攻擊(3)

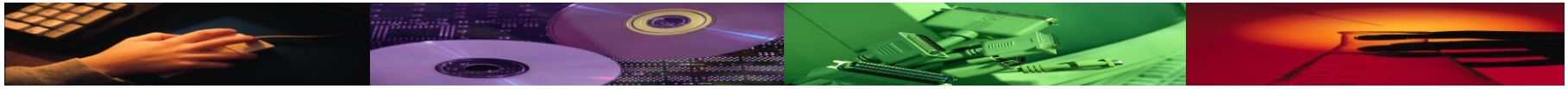


知名的供應鏈攻擊事件 (Jul-2021)

- ◆ Kaseya : IT 管理、遠端監控軟體公司
  - 加密勒索金錢



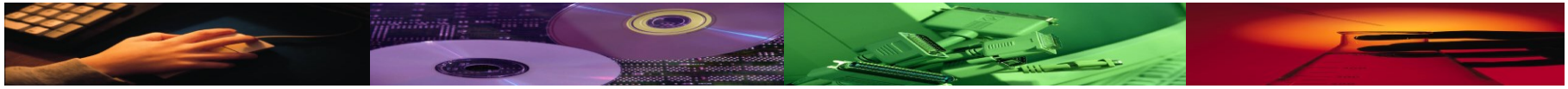
資料安全威脅



摘要說明

- 針對資料源的系列威脅，未經授權存取資料、揭露資料、發佈虛假資訊。
- 網路攻擊、內部人員、意外遺失或資料曝露都會導致資料洩漏。
- 資料滲出或資料竊取是攻擊者用來定位、複製和傳輸敏感資料的一種技術。
- 資料滲出的一種特殊狀況是身分盜用，攻擊者使用受駭者的個人身分資訊來冒充。

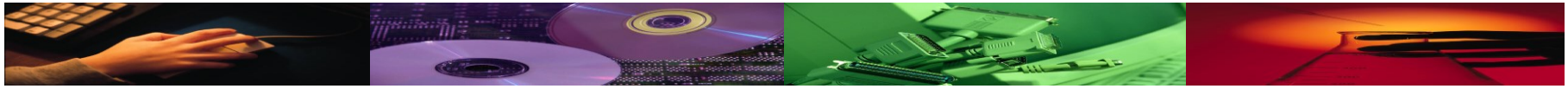
資料安全威脅的趨勢分析



- 人為錯誤是資料洩漏的主要原因。
- 醫療保健行業的資料洩漏激增。
- 商業環境中的資料洩漏事件增多。
- 攻擊動機和攻擊強度保持不變。

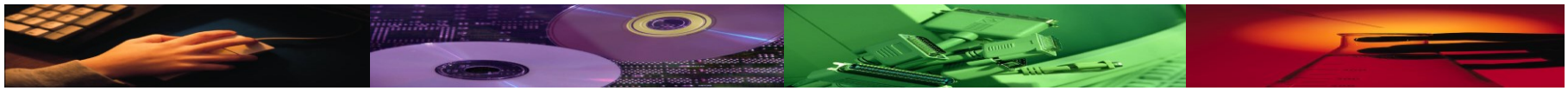
https://learngxp.com/

資料安全威脅的因應方式



- 資料識別和分類
  - ✓ 類型、位置、使用者
  - ✓ 敏感和需要保護的資料
- 認證和授權
  - ✓ 例如：多因子驗證
- 資料安全稽核
  - ✓ 例如：滲透測試
- 反惡意軟體、反垃圾郵件、反病毒和端點保護

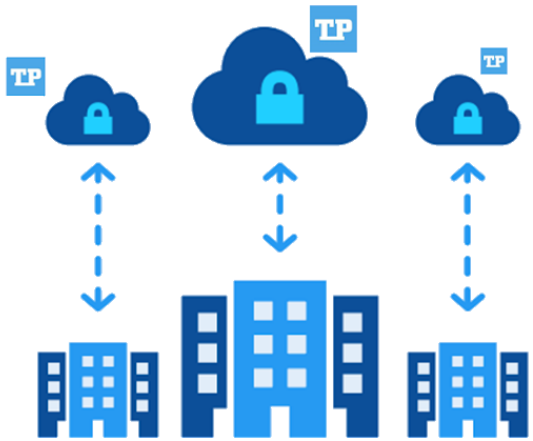
雲端環境威脅



摘要說明

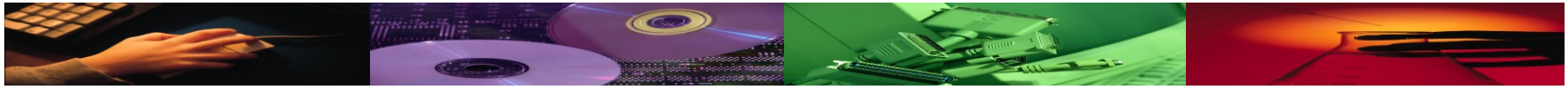
- 雲端服務現在是許多業務流程的關鍵要素，簡化文件共享和協同作業。
- 隨著越來越多企業會走向混合辦公環境，網路犯罪和有針對性的攻擊者常使用雲端服務漏洞利用、將雲端服務用於惡意軟體託管和 C2 中繼站，以及利用配置錯誤的鏡像容器。

公有雲 : 服務由第三方提供、資料由第三方保管



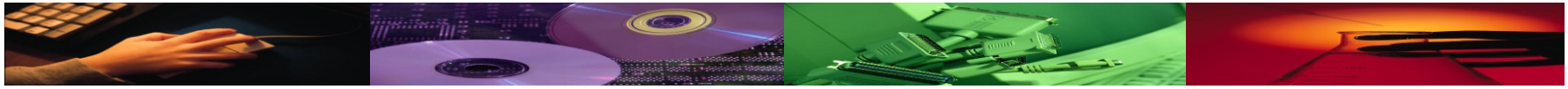
私有雲 : 企業專屬的雲端服務、服務及資料自主管理

雲端環境威脅的趨勢分析



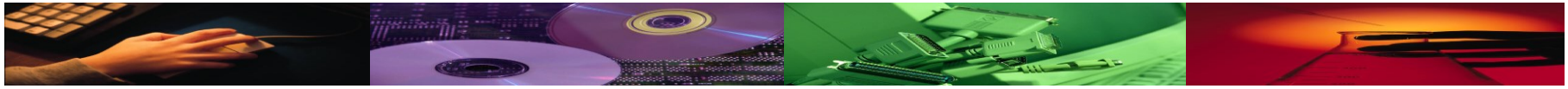
- 雲端平台漏洞利用增多
- 無法掌握情況
- 設定錯誤、存取權限管理
- 惡意軟體託管和中繼站部署
- 五大要素決定選用的雲
  - ✓ 延遲性
  - ✓ 資料頻寬
  - ✓ 獨立性
  - ✓ 隱私性
  - ✓ 與本地資源的互動性

雲端環境威脅的因應方式



- 防火牆設定別偷懶
- 金鑰存取權限設定要做好
- 機敏資訊要守好
- 帳單預算通知要設定
- 多層防護保心安

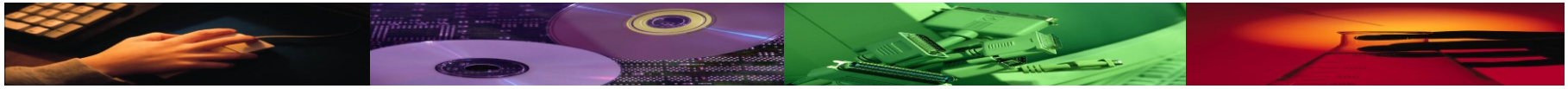
勒索軟體攻擊



摘要說明

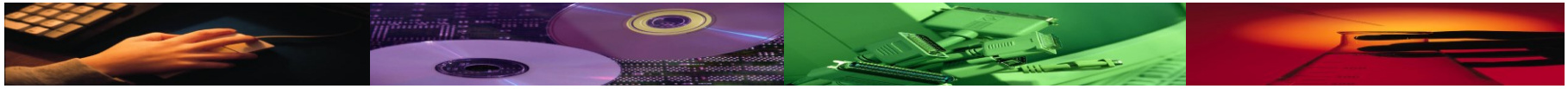
- 針對基礎設施的勒索軟體攻擊顯著增加。
- 幾乎日常生活各方面都是到勒索軟體的威脅，包括醫院、警局、自來水廠、燃料管道、食品製造和學校。
- 遇到這類攻擊，企業不僅要支付鉅額的贖金，將會面臨媒體報導和政府審查，讓企業不僅面臨經濟損失，更是聲譽受損。

勒索軟體攻擊的趨勢分析



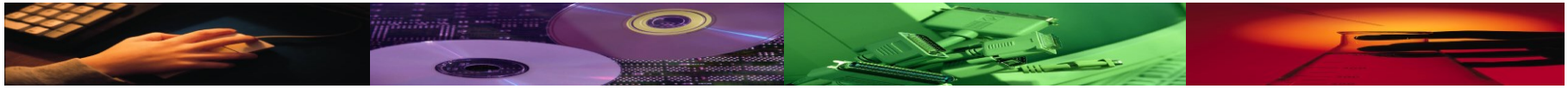
- 勒索軟體組織針對基礎設施發動攻擊
- 遠端桌面連線和釣魚郵件依舊是最常見的攻擊方式
- 利潤最大化：從雙重勒索到多重勒索的轉變
- 勒索軟體及服務(RaaS) 商業模式發展壯大
- 招募企業員工協助攻擊

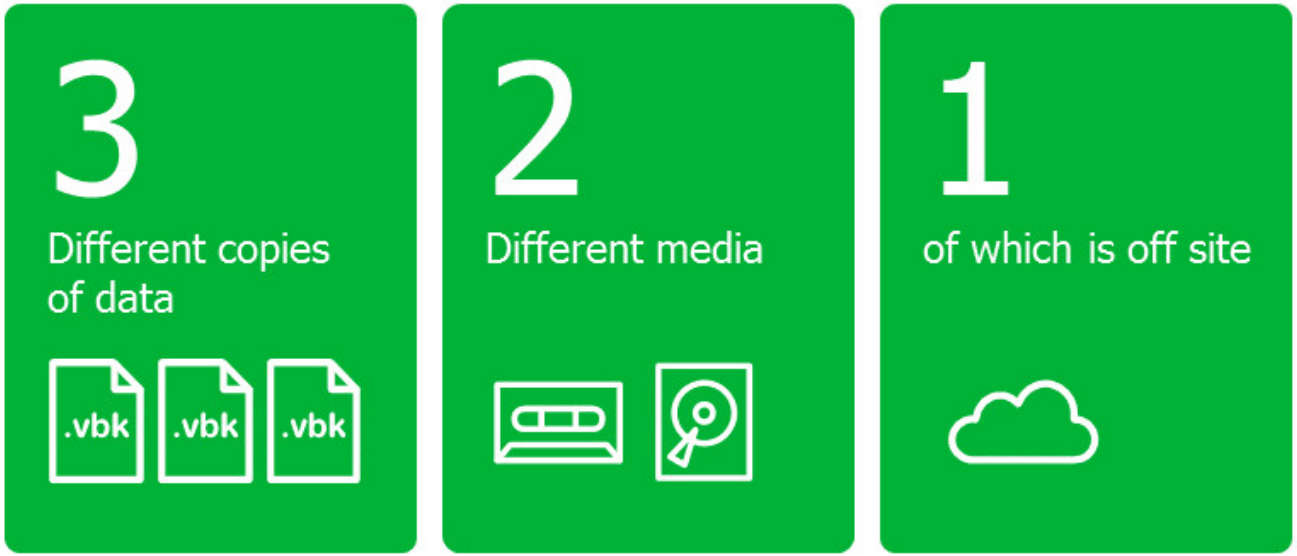
勒索軟體攻擊的因應方式



- 保持良好的網路習慣。
- 及時向主管單位報告。
- 做好資料備份。
- 定期進行修正程式更新。
- 最簡單的，往往也是最有效的。

備份321原則

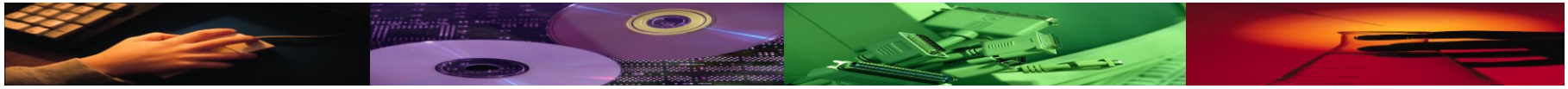




- 至少3份備份
- 分別儲存在2種不同儲存媒體
- 至少1份放在異地保存

- 越是重要、敏感、風險高的資料，就需要越頻繁的備份，甚至在重大異動之前，得先把資料備份，以免異動出事後，無法將資料復原。

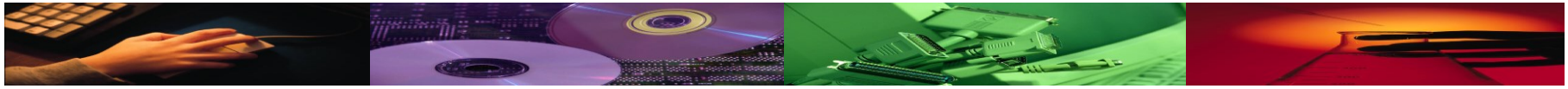
漏洞利用攻擊



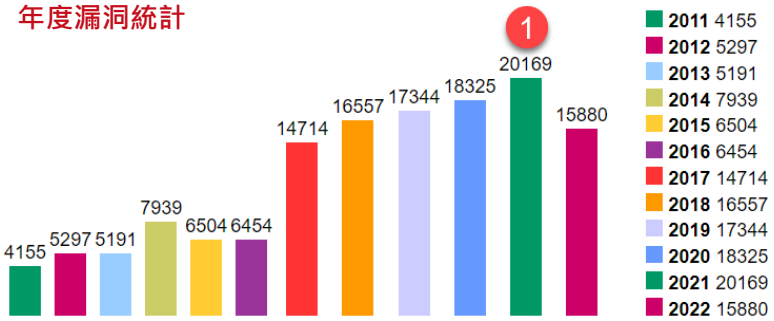
摘要說明

- 漏洞利用是資訊系統中缺乏防控措施或是防控措施不足所造成。
- 因為漏洞直接影響安全核心-系統權限，所以備受攻擊者青睞。
- 美國、澳洲、加拿大、紐西蘭與英國等5個國家的網路安全機構公布了2022年最常遭到駭客利用的安全漏洞。
  - ✓ 6個屬於遠端程式攻擊漏洞，分別是存在於微軟Exchange Server的CVE-2021-34473，位於Zoho ManageEngine ADSelfService Plus的CVE-2021-40539，出現在Apache Log4j2的CVE-2021- 44228，現身於VMware Workspace ONE存取暨身分管理功能中的CVE-2022-22954，微軟多個產品中的CVE-2022-30190，以及Atlassian Confluence Server and Data Center的CVE-2022-26134。
  - ✓ 當中最老的漏洞是出現在FortiOS與FortiProxy中的CVE-2018-13379，且駭客也曾公布來自全球74個國家、近50萬組的Fortinet VPN登入憑證

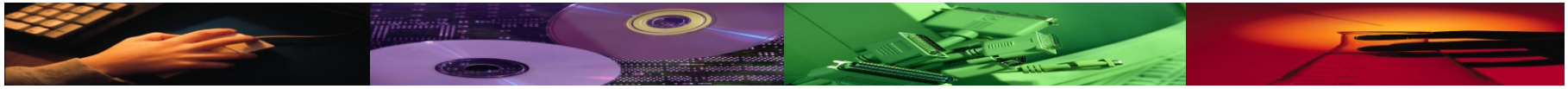
漏洞利用攻擊的趨勢分析



- 2021年公開的 CVE 首次超過 20,000 件
- 重蹈覆轍：被攻擊者利用的前 10 個漏洞有 8 個是原廠已經釋出修正程式或更新版本的漏洞
- 史詩級漏洞 Log4j 席捲全球
  - ✓ 比利時 國防部因此漏洞受到駭客威脅

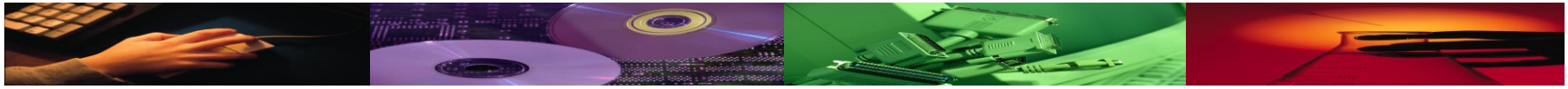


勒索軟體攻擊的因應方式



- 更新軟體版本或採臨時變通的紓解措施
- 優先修正在網際網路上提供的資訊服務
- 重點修復攻擊者最常利用的漏洞
- 從外部訪問內部網路時，務必要採用多因子身分認證，尤其是系統管理員或特權帳號
- 以縱深防禦戰術輔以威脅情報來取代基於邊界的安全防護

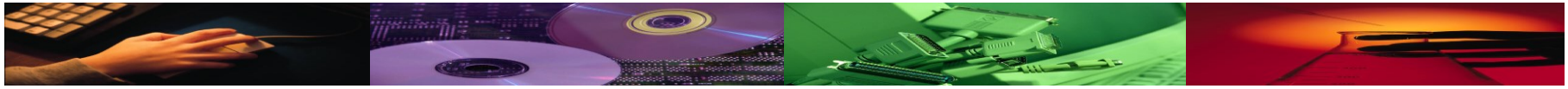
挖礦劫持攻擊



摘要說明

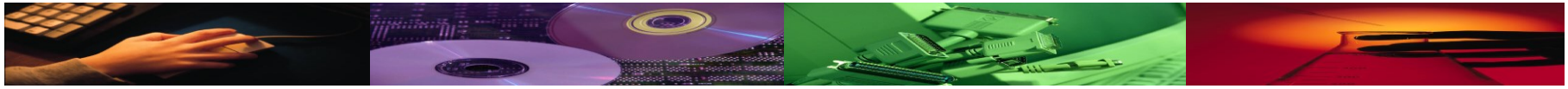
- 駭客偷偷使用受害者電腦的計算能力來獲取加密貨幣的一種網路攻擊形式。
- 藉由使用者電子郵件的網頁連結或誘導使用者存取受感染的網站。
- 挖礦劫持常進化成更複雜的攻擊，包括資料洩漏、鍵盤紀錄和信用卡資訊竊取。

挖礦劫持攻擊的趨勢分析



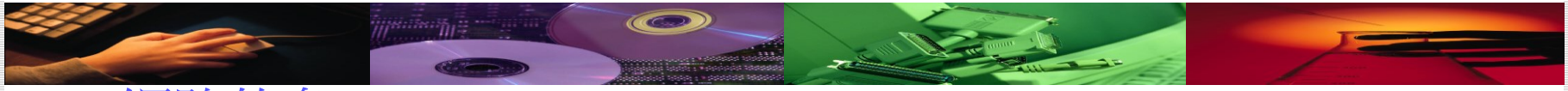
- **2021年加密挖礦劫持數量創歷史新高**
- **XMRig (開源挖礦程式)主導整個礦幣市場**
  - ✓ XMRig(51%)、Lucifer(10%)、LeminDuck(5%)、RubyMiner(5%)、Wannamine(5%)、Other(20%)
  - ✓ 2021年4月 XMRig 透過漏洞以來植入微軟郵件伺服器 (Microsoft Exchange Server)
- **從瀏覽器轉為基於文件的加密劫持**
  - ✓ 瀏覽器(13%)、文件(87%)
- **挖礦劫持攻擊目標轉移**
  - ✓ 雲端服務及容器基礎設施

挖礦劫持攻擊的因應方式



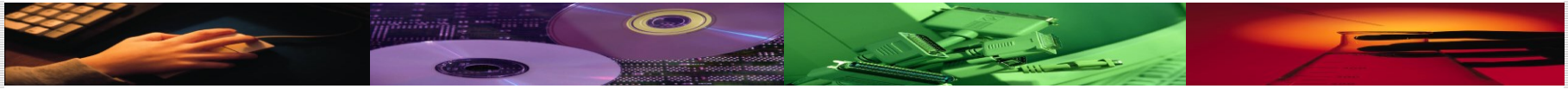
- 安全意識培訓
  - 釣魚郵件、水坑式攻擊
- 廣告攔截
- XMRig (開源挖礦程式)主導整個礦幣市場
  - XMRig(51%)、Lucifer(10%)、LeminDuck(5%)、RubyMiner(5%)、Wannamine(5%)、Other(20%)
  - 2021年4月 XMRig 透過漏洞以來植入微軟郵件伺服器 (Microsoft Exchange Server)
- 文件完整性監控
- 終端保護
  - NGAV、EDR

10種常見社交工程攻擊手法(一)



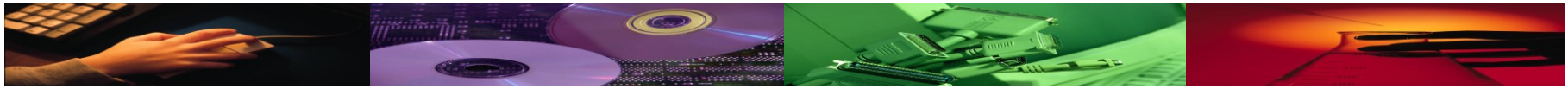
- 網路釣魚(phishing)
  - 最普遍，使用假電子郵件、網站和短信從**毫無戒心**的受害者…。
  - **五分之一的員工**仍然會點擊這些可疑連結。
- 魚叉式網絡釣魚(Spear Phishing)
  - 針對特定目標進行攻擊。
- 下餌(Baiting)
  - 使用吸引力誘餌…取得敏感資料。
- 惡意軟體(Malware)
  - 嚇唬您…讓您採取行動，使用危險警告來報告虛假惡意軟體感染或聲稱您的帳戶已被洩露，例如勒索軟體。
- 假託(Pretexting)
  - 類似網路釣魚，冒充成您的朋友、同事、家人…，角色扮演、營造出完整的情境進行欺騙。

10種常見社交工程攻擊手法(二)



- 等價交換(Quid pro quo)
  - 以資訊或服務交換為中心，以說服受害者採取行動。
- 尾隨 (Tailgating)
  - 跟著其他人，利用他們的憑證來進入限制區域。
- 電話網釣(Vishing)
  - 將電話號碼偽造成您信任的機構，然後使用預錄語音、或用文字轉語音合成器來掩飾身份(例如...電話費尚未繳)
- 水坑(Water-Holing)
  - 不是去攻擊目標，而是去埋伏在目標必經之路。
- 交友詐騙（Catfishing）
  - 利用別人的照片、影片和個人資料建立一個虛假的社群帳號，這些假身份通常用於網路霸凌或尋求關注。

課程大綱

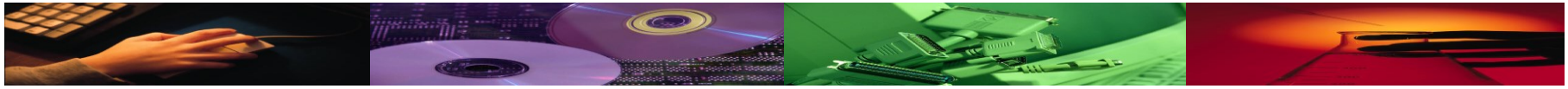


我們與駭客的距離

認識資安問題

建立應對技能

這樣上網很危險



打開來歷不明的網頁、電子郵件鏈結或附件

電腦不裝防毒軟體

不更新防毒軟體及常用的應用程式

經常瀏覽成人網站、色情網站

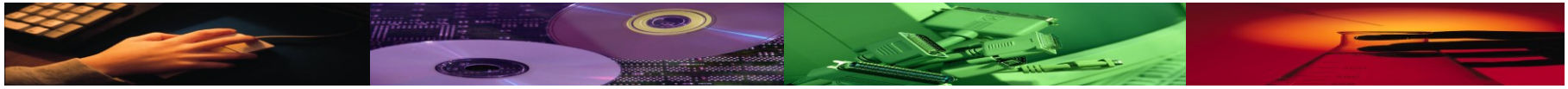
點擊查看低價或免費商品廣告

在多個系統服務使用相同密碼，密碼強度弱

相信輕鬆賺大錢，掉進網路傳銷陷阱

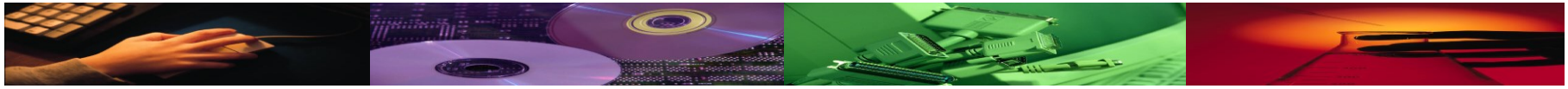
隨意連結公共場所免費 WIFI

企業/學校/機關 常面臨的三大威脅



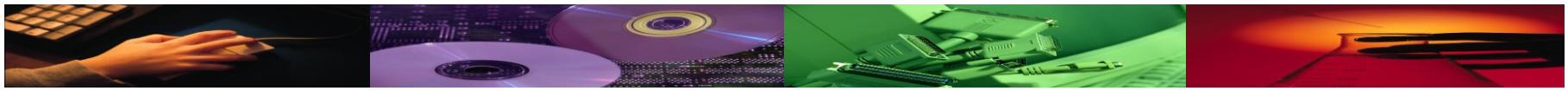
- 都與『人員風險』有關。
- 企業/學校/機關面臨的最三大威脅。
  - ✓ 網路釣魚攻擊位居榜首。
  - ✓ 商務電郵詐騙 (BEC) 攻擊或稱變臉詐騙攻擊位居第二。
  - ✓ 勒索軟體位居前三。
  - ✓ 前三名中有兩個依賴於社會工程策略，雖然勒索軟體攻擊可以通過腳本漏洞利用實現自動化，但也經常會利用社會工程策略或勾結內部人員。
- 絕大多數勒索軟體攻擊也都是從網路釣魚電子郵件或利用弱密碼開始的。

數位資訊的世代，如何保護您自己



1.電腦鎖定畫面
2.好用的手機 APP
3.雲儲存安全使用
4.手機維修/報廢
5.外出辦公安全
6.辦公通訊安全
7.會議安全
8.Bad USB
9.桌面便利貼
10. 安全意識薄弱的特定人群
11. 公用 Wi-Fi 風險
12. 私架 Wi-Fi 熱點
13. Wi-Fi 共用軟體
14. 惡意軟體後門
15. 物聯網弱密碼及漏洞
16. 社交軟體送貨上門
17. 人臉資訊被濫用
18. 填問卷送大獎
19. 盜版軟體
20. 遠端連線軟體
21. 公用密碼
22. 更新不是騙人的
23. 固定會議密碼
24. 好奇心害死的不只是貓
25. 測試你的密碼弱不弱
26. 不要亂掃二維碼

1.電腦鎖定畫面



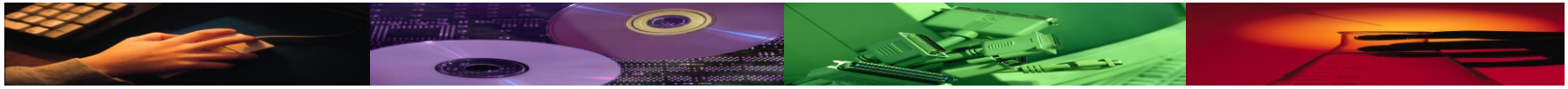
案例解析

- 同事間的工作性質與內容不同，有權看到的資訊級別也不同，在開放的辦公環境，有可能來自外部門或外組織的人員。
- 長時間離開電腦前，經過的人不光能看到螢幕內容，別有用心的人還會開啟並複製電腦中的各種檔案。

安全提示

- 電腦設置螢幕保護裝置，避免離開時忘記鎖定電腦。
- 短時間離開電腦前要鎖定電腦。
- 長時間離開電腦前建議關機。
- 提高使用電腦安全意識，一定要設置開機密碼。

2.好用的手機APP



□ 案例解析

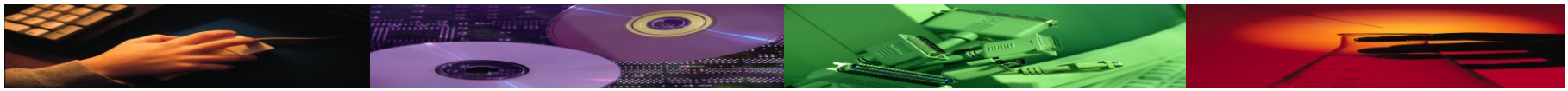
- ✓ 若手機近期出現手機出現異常發燙、耗電速變快、佔用網路流量，很有可能是被藏有惡意木馬程式的APP入侵。
- ✓ APP名稱會偽裝成的工具類的軟體，以解鎖全部功能或禁用應用內廣告為藉口，要求使用者登入 FB 帳戶，藉此竊取個資 (帳號、密碼和其他授權)。

Google Play

□ 安全提示

- ✓ 檢視 APP 要取得的權限。
- ✓ 安裝正版且具知名度的手機防毒軟

3.雲儲存安全使用



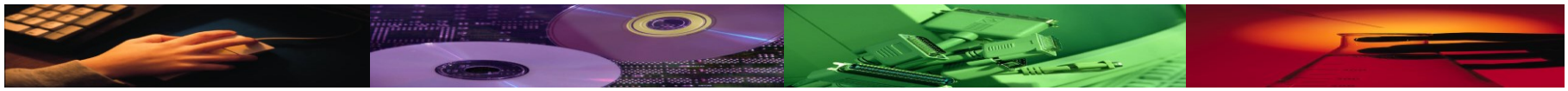
案例解析

- 雲端硬碟為機構和個人提供資訊的存儲、讀取、下載等服務，存儲量大，應用簡便成為了大眾喜愛的存儲方式，但也容易成為駭客攻擊的目標。
- “技術賊”利用專業技能破譯密碼，WI-FI釣魚，同時雲端硬碟本身可能存在的漏洞被利用。

安全提示

- 在雲儲存應用過程中設定時間維度，並及時清理檔。
- 不與他人共用使用 ，不存儲機密檔案。
- 行動端使用關閉自動備份功能。
- 中國科技巨頭如阿里巴巴、字節跳動、騰訊等，已經將網路演算法細節資訊交給中國監管機構。

4.手機維修、報廢



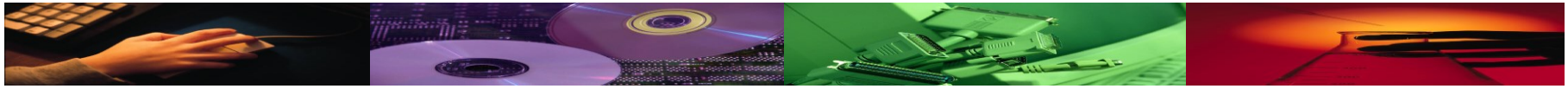
案例解析

- 在更換手機後，將舊手機恢復出廠設置是必要的，但也只是把系統檔簡單還原、使用者資料簡單刪除，在手機晶片上並未徹底刪除。
- 系統「復活」對於技術人員是「零門檻」
  - 通話記錄、簡訊、聯繫人、多媒體文件、第三方支付紀錄、郵件訊息

安全提示

- 手機出售前注意事項
  - 刪除社交APP的登錄設備，退出APP原有帳號
  - 清除所有數據，把手機恢復原廠設置
  - 用大的影音檔案完全複寫反覆複製刪除幾次

5.外出辦公安全



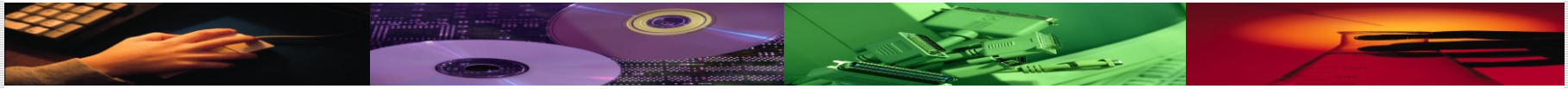
案例解析

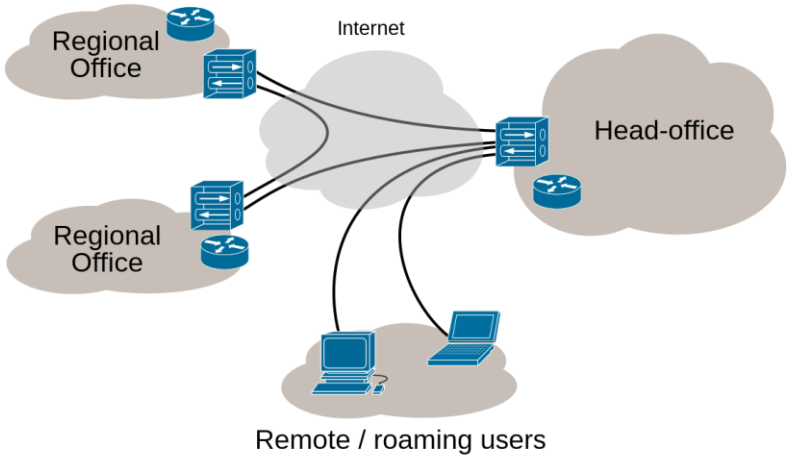
- VPN 為通過一個公用網路建立一個臨時的、安全的連接，是一條穿過混亂的公用網路的安全、穩定隧道，使用這條隧道可以對資料進行加密達成安全使用的目的。

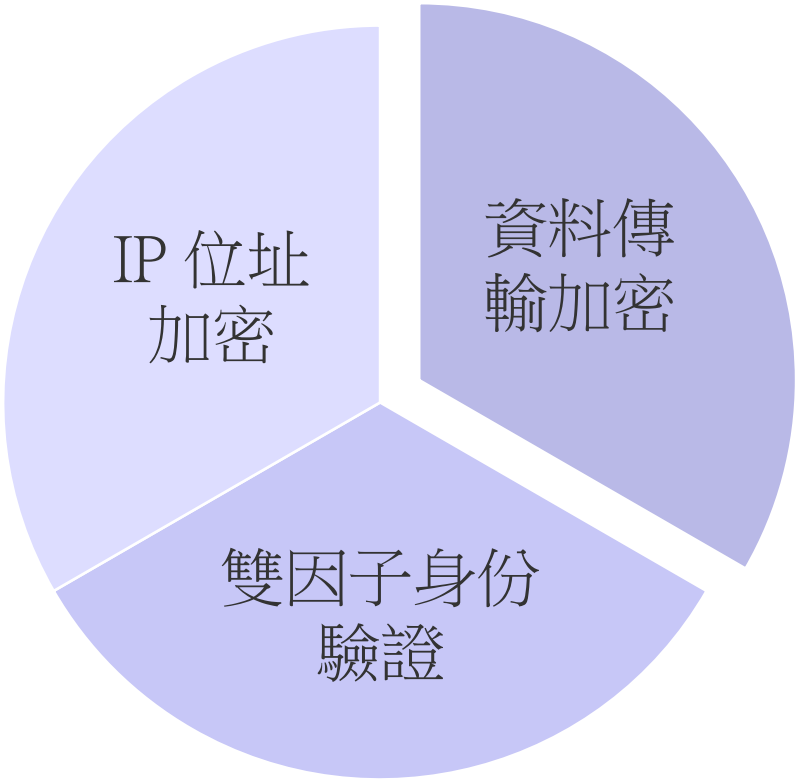
安全提示

- 組織內部資料應建立內部伺服器資源，便於員工應用，且降低遺失、盜用的風險。
- 建立 VPN 系統，無論員工出差或在家中都能時刻訪問內網資源。

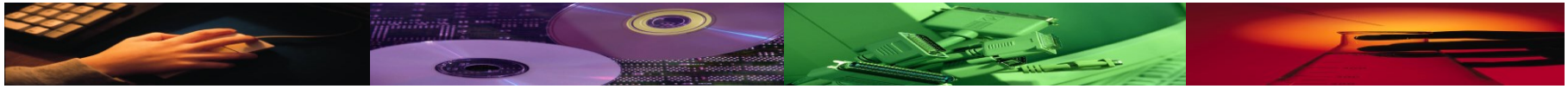
VPN連線安全管理







6.辦公通訊安全

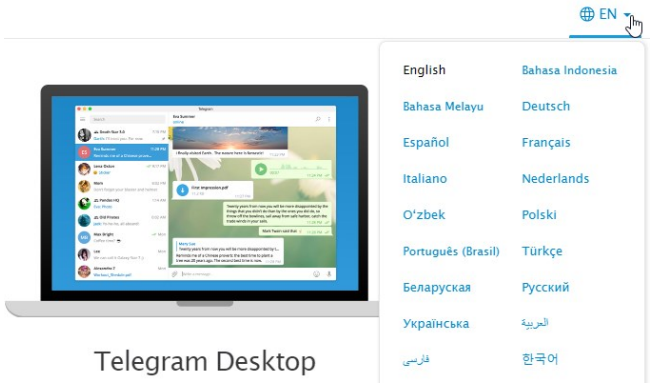


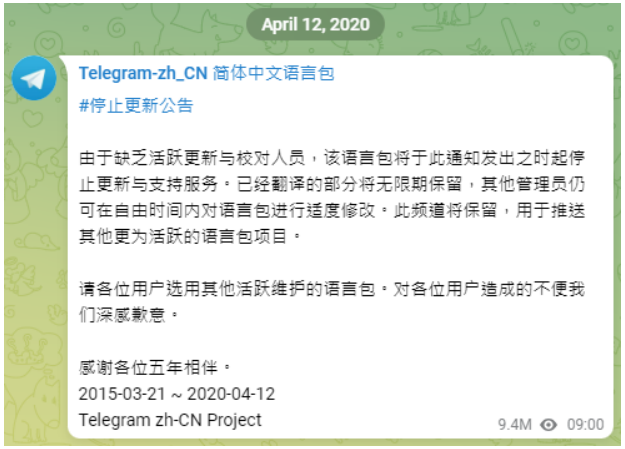
案例解析

- ✓ 網際網路應用讓溝通更便捷，同時也帶來了很多網路安全隱患。
- ✓ 通訊軟體 Telegram 尚未支援中文，因此有熱心網友提供簡體中文語言包。
- ✓ 簡體中文語言包團隊早已停止繼續維護，駭客利用語言包植入木馬程式。

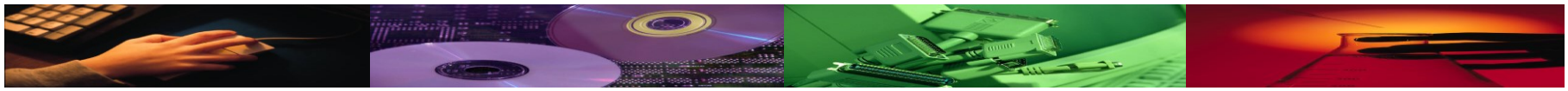
安全提示

- ✓ 在溝通交流前，首先做好重要文件的備份。
- ✓ 對重要、敏感檔進行加密，避免被直接利用。
- ✓ 在工作溝通與日常社交工具區分開。



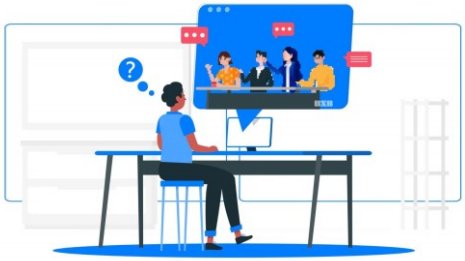


7.會議安全



案例解析

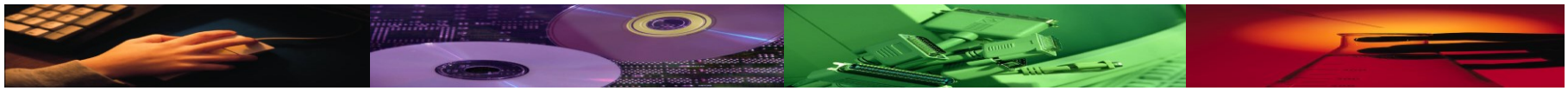
- ✓ 會議進程中會經常用到白板，記錄、整理主要論點、思路及核心資料。
- ✓ 在開會進程中，要保證會議場地的資訊安全性，參會人員可靠性，知情權等級，稍有不慎則有可能被非授權人無意識聽到、看到，並且有意識或無意識的傳播。
- ✓ 線上會議未設定存取權限。



安全提示

- ✓ 重要會議，選擇隔音效果好的會議室
- ✓ 會議期間拉緊窗簾或關閉門窗。
- ✓ 重要會議禁止拍照、錄音等行為。
- ✓ 會後及時清理白板，桌面檔，多媒體設備存檔。
- ✓ 重要線上會議設定存取權限。

8.Bad USB

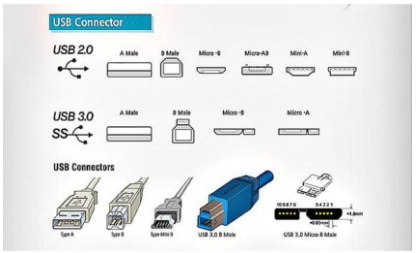


案例解析

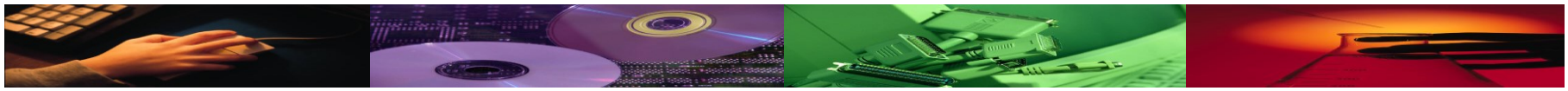
- ✓ 經過重寫 USB 韌體偽裝成 USB 輸入設備(如滑鼠、鍵盤、網卡)用於惡意用途的 USB 設備。
- ✓ 防毒軟體對此類硬體攻擊防禦效果較差。
- ✓ 隨意在辦公電腦插入來源不明的USB設備，就會有電腦被入侵的可能。

安全提示

- ✓ 對人資、研究、財務等敏感區域，通過管理和技術性措施限制行動儲存設備使用，並定期檢查。
- ✓ 使用終端安全軟體的U盤控管和封堵功能，對類似行為進行告警和封鎖。
- ✓ 不在電腦上使用來源不明的 USB 設備，包括小檯燈、資料傳輸線等等。

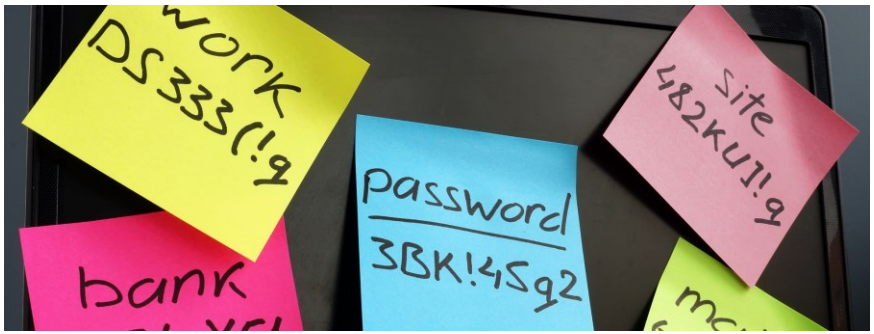


9.桌面便利貼



案例解析

- 桌面或便利貼紀錄代辦和密碼很方便，但很容易被無關人員看到或在無意間流出，導致資訊洩漏的風險。

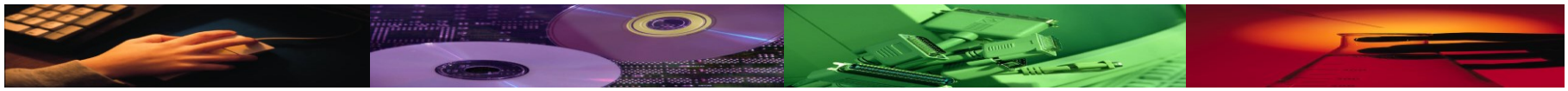


安全提示

- 敏感文件放入帶鎖的抽屜或櫃子。
- 避免在桌面上放置敏感檔、儲存敏感資訊的設備、門禁卡、寫有密碼的便利貼。
- 使用 Keepass 等密碼管理工具或手機備忘錄功能紀錄敏感事項。

KeePass
Password Safe

10.安全意識薄弱的特定人群



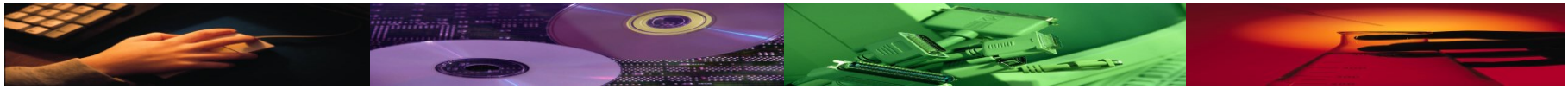
案例解析

- 對於員工、能夠進出辦公區域、或對組織有足夠瞭解的協力廠商人員(如保全)網網友容易被利用進行資訊獲取或攻擊。

安全提示

- 安全意識教育要包括所有有權限進入辦公區的人。
- 從管理措施上避免 Wi-Fi密碼分享、敏感檔未經銷毀即直接丟棄。

11.公用 Wi-Fi 風險



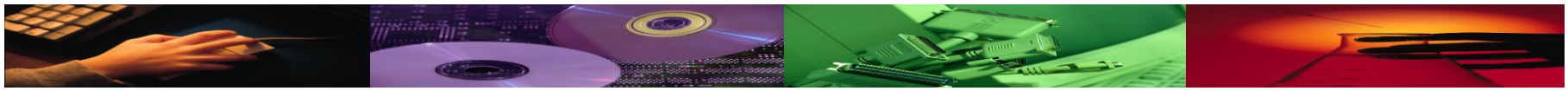
案例解析

- 在公共場所，通常部署免費的 Wi-Fi 。
- 攻擊者可能會建立具迷惑性的 Wi-Fi 熱點， 一旦沒留意連接到這些惡意熱點，可能會導致資訊洩漏、流量劫持等風險。

安全提示

- 在公眾場所連接 Wi-Fi 前，應留意周圍的提示，接入官方提供的網路 。
- 在處理敏感資訊或進行行動支付時，最好使用個人的行動網路 4G、5G，儘量不要使用公用網路。
- 不需要使用 Wi-Fi 和藍芽時，將手機的 Wi-Fi 和藍芽功能關閉。

12.私架 Wi-Fi 熱點



案例解析

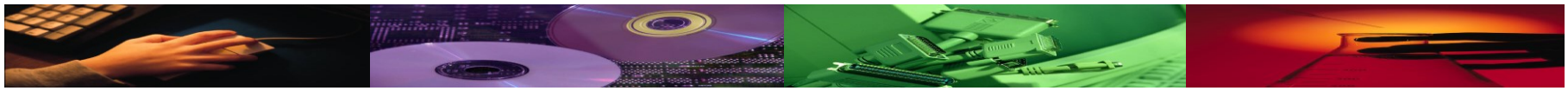
- Wi-Fi 信號具有一定的覆蓋範圍，不僅在工作區域可以連接，甚至在附近的區域也可以連線。
- 私自架設的 Wi-Fi 加密方式禿長較弱，一旦被攻擊者成功破解，可能會導致攻擊者直接訪問內部網路的風險。

安全提示

- 在辦公區域，使用組織提供的網路接入方是，不要自行搭建個人熱點，不要使用”Wi-Fi 分享器”設備。
- 如果確有需要，在架設無線路由器前必須經過組織核准，並進行安全檢查。
- Wi-Fi 應使用安全演算法，設定複雜強勢密碼，保證密碼定期更改。

弱密碼　25米傳輸距離　設備漏洞

13.Wi-Fi 共用軟體



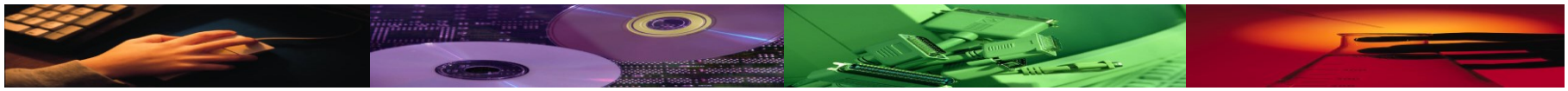
案例解析

- Wi-Fi密碼共用類App 會在安裝後自動上傳所有連接過的 Wi-Fi密碼，其中很可能也包含家庭、工作機構的密碼。
- 一旦攻擊者使用這類工具，可以輕易地連接到家庭或工作機構的網路。

安全提示

- 儘量避免使用 Wi-Fi密碼共用類 App。
- 如果需要使用，關閉自動上傳密碼功能。

14.惡意軟體後門



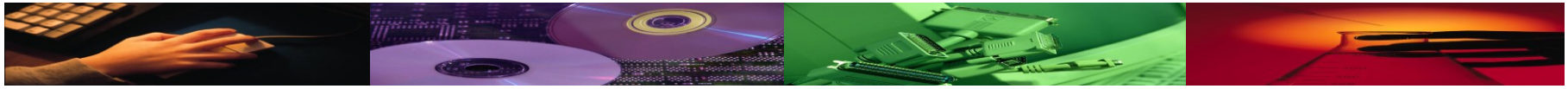
案例解析

- 非法軟體會自動開通許多權限，大量收集電腦和使用者資訊，用來出售隱私資料，甚至進行勒索。

安全提示

- 不要在手機上下載非法軟體或來源不明的App，避免安全和隱私洩漏問題。
- 設定軟體自動更新，安裝防毒軟體。

15.物聯網設備弱密碼及漏洞



案例解析

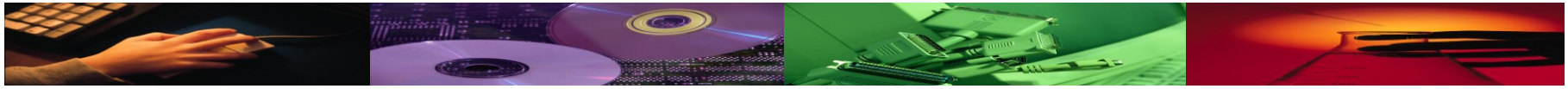
- 家用攝影機等物聯網設備，常常存在預設密碼。
- 物聯網設備可能存在各類漏洞，可能會被攻擊者輕易破解利用。

大華科技 app： GDMSS	帳號:admin	密碼: dh123456
海康威視app： IVMS-4500	帳號:admin	密碼: 888888 or hk888888
昇銳電子app： Super Live Plus	帳號:admin	密碼: 123456
雄邁 app： vMEyePlus	帳號:admin	密碼:空白
馥鴻app： vacronViewer	帳號:admin	密碼:空白
環民 app： Aquila	帳號:admin	密碼: 123456
可取app： SoCatch	帳號:admin	密碼: 123456
杭特app： IPMOTION LITE	帳號:admin	密碼: admin

安全提示

- 物聯網設備接入家庭局域網時，注意關閉網路對外共用功能，修改預設密碼。
- 盡量購買規模較大、具有良好聲譽的廠商所製造的物聯網產品，及時根據廠商售後提示對物聯網設備進行升級。

16.社交軟體送貨上門



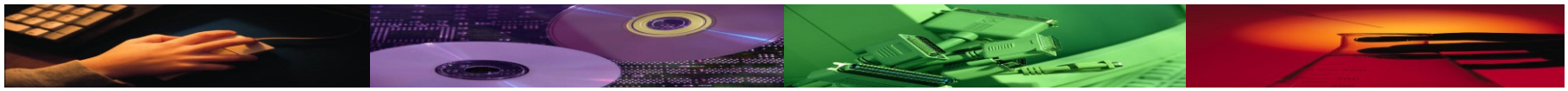
案例解析

- 社群軟體中發布的資訊，往往包含個人真實生活的寫照。
- 分享之餘更要注意個人隱私的保護。

安全提示

- 在社群軟體平臺，不要發布包括個人可以識別資訊的圖文，包括姓名、地址、身分證號、組織職務
- 通訊進階加密(設定-隱私設定)
- 登入中的裝置(設定-我的帳號)

17.人臉資訊被濫用



案例解析

- 身份證照片、沒有標示用途的身份證影印本、人臉識別等隱私資料，可能因為軟體漏洞、內部惡意員工等途徑被不法份子收集，濫用進行帳號註冊、貸款、詐騙、深偽技術(Deepfake)等違法活動。

安全提示

- 對服務商非必要使用人臉識別的場景，消費者有權不接受人臉識別。
- 使用身份證影印本時，最好在複印件上標示用途，不要輕易洩漏和發送給別人，避免被不法分子濫用。

18.填問卷送大獎

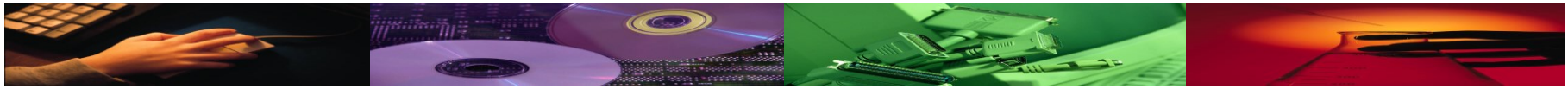
案例解析

- 製作問卷的程式門檻極低，不法份子常用這種方法去誘導使用者填寫個資。

安全提示

- 天下沒有白吃的午餐，遇到需要填寫個人資料的場景需特別留意。
- 對個人資料分類分級，身份證字號、居家地址、健康狀況等資訊不要透漏給無關第三者。

19.破解軟體



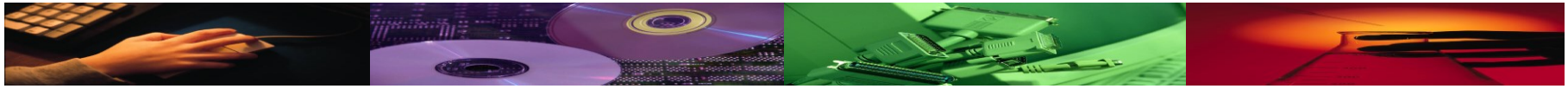
案例解析

- 駭客利用軟體下載(免費版、破解版)網站，將病毒、廣告捆綁後進行分發
- 提示用戶關閉防火牆或授權等錯誤行為
- 惡意程式下載挖礦模組、蒐集瀏覽器、 IG 與 FB資訊，竊取信用卡/支付憑證

安全提示

- 購買正版軟體
- 到官方網站下載
- 對於無法識別軟體，請聯繫資訊服務處進行申請使用

20.遠端連線軟體

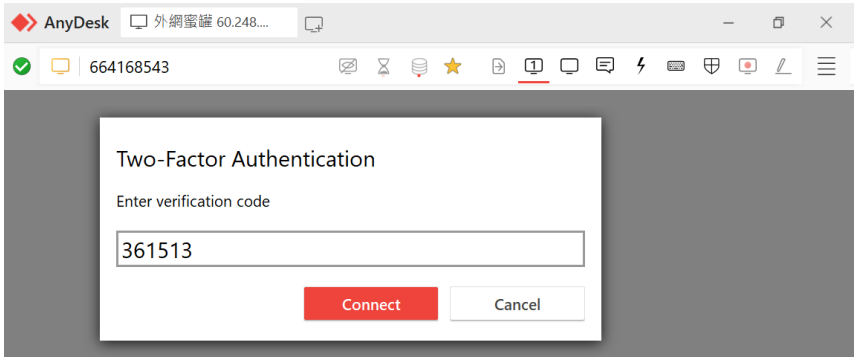


案例解析

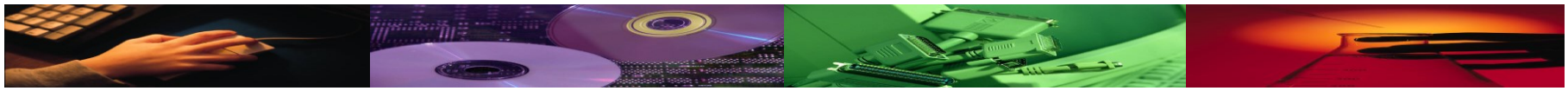
- ✓ 為了方便把遠端連線軟體設定為固定驗證碼，但是在遠端完成協助後忘記變更密碼，就會對電腦甚至內網帶來威脅。

安全提示

- ✓ 機關內部管制遠端連線軟體。
- ✓ 使用官方釋出的遠端連線軟體。
- ✓ 安全性設定 - 導入雙重認證。



21.公用密碼

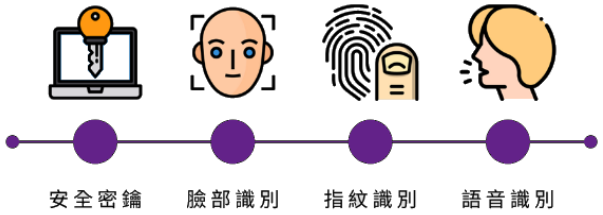


案例解析

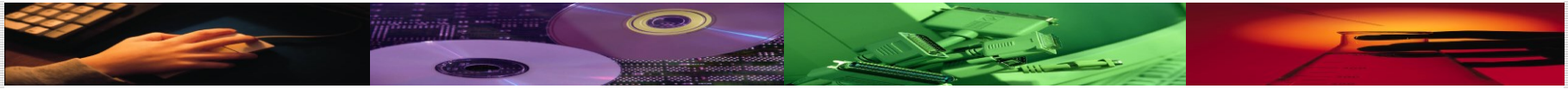
- 撞庫是駭客通過收集已洩漏的帳號和密碼資訊，嘗試登錄其他網站。
- 通用密碼極易受到撞庫攻擊的威脅

安全提示

- 最安全的方式是針對每一個網站或系統設定不同的密碼。
- 如果擔心忘記，可先記住一個基礎密碼，再加上不同網站/系統各自的代號。
- 導入 FIDO (Fast Identity Online) 機制，透過生物特徵註冊一把鑰匙，透過這把鑰匙暢行網站與應用服務。



免費的最貴



STARBUCKS

星巴克免費Wi-Fi

使用條款

使用無線網路前請先閱讀使用條款：

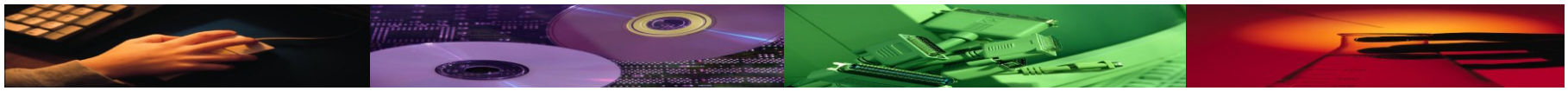
一、使用者行為規範 本服務專供使用者作正常合法網路通訊之用，不應以任何方式轉供商業用途，不得影響其他使用者及本公司權益，並應遵守中華民國相關法規及一切使用網際網路之國際慣例。 就使用者使用本服務所為行為，本公司並無監督管控義務，其所生之相關法律責任均由使用者自負，必要時本公司得報請相關單位依法裁處。 使用者有下列情形之一者，本公司有權暫停或終止其使用本服務，使用者不得要求賠償：

1. 竊取、更改、破壞他人資訊者。
2. 擅自複製他人資訊轉售、轉載者。
3. 危害通信或影響其他使用者權益者。
4. 未經他人同意，擅自寄發電子訊息至他人信箱造成困擾者。
5. 於論壇區張貼與主題無關之訊息者。

接受並繼續

免費的最貴~

22.更新不是騙人的



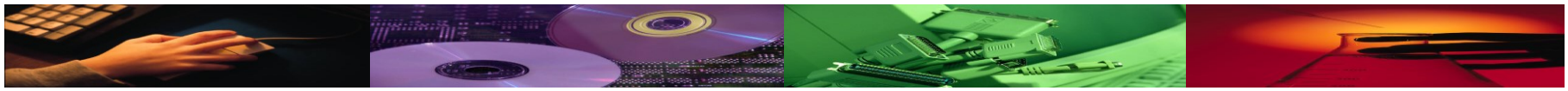
案例解析

- 作業系統和軟體不可避免會出現各類漏洞，**安全更新正是對漏洞的修補**。
- 在修正程式公佈後，攻擊者可能會據此反推漏洞的利用方式，在使用者還沒來得及升級更新的這段時間發出攻擊。
- 先前爆發的各類挖礦勒索病毒大多如此。

安全提示

- 建議開啟作業系統和各類應用程式的自動安裝更新功能，或在有更新時發出通知提示。
- 修正程式發布後，應第一時間進行更新，更新完成後確認安裝是否成功。
- 駭客針對重大的漏洞，在原廠發佈修正程式當天，即完成漏洞利用程式並著手進行入侵。

23.固定會議密碼



案例解析

- 視訊會議僅通過會議識別碼、密碼或鏈結形式登入，無法有效確認和控制餐會人的身分與行為。
- 存在錄製、拍照、無關人員參會的風險。

Microsoft Teams 會議

在您的電腦或行動裝置應用程式上加入

按一下這裡以加入會議

或輸入會議室識別碼加入

會議識別碼: 447 537 807 245

密碼: BMT9wT

或撥入 (僅限語音)

+886 2 7752 4099,,355854521# Taiwan, Taipei

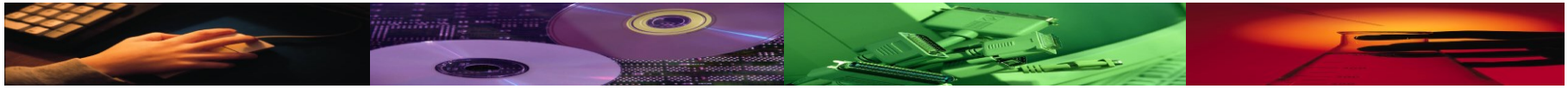
電話會議識別碼: 355 854 521#

尋找當地電話號碼 | 重設 PIN

安全提示

- 使用會議識別碼、密碼的形式申請線上會議。
- 會議發起人在會前通知時應將會議識別碼、密碼發送給需要參加的人員，並告知會議紀律。
- 要求參會人必須實名登錄， 開啟鏡頭。

24.好奇心害死的不只是貓



□ 案例解析

- ✓ 駭客常常引誘使用者訪問惡意釣魚鏈結點擊執行惡意程式，進而入侵電腦。
- ✓ 駭客常常會經由加密附件或壓縮檔案繞過郵件防護。

From: 中華郵政全球資訊網 <info@reforco-morioka.jp>
Sent: Friday, October 1, 2021 7:46 AM
To: [redacted]
Subject: 嘗試投遞; 錯誤的地址

親愛的收件人：

為了送遞包裹，編號 RF618024878TW，我們需要您採取其他行動。
由於我們的送遞員無法到達此位置，因此為此包裹提供的送貨地址不正確或不存在。

由於此送遞嘗試失敗，因此包裹已退回我們的倉庫。
在這裏，您可以選擇幾種不同的選項：

□ 安全提示

- ✓ 對於內容有網址鏈結、加密檔或壓縮檔案的郵件要特別留意。
- ✓ 使用郵件防護系統，對風險即時監測並阻斷。

https://bee2bee.hr/gret
按住 CTRL 鍵再按一下滑鼠以追蹤連結

>> 更新提供的送遞地址
>> 安排將包裹送遞到其他地址

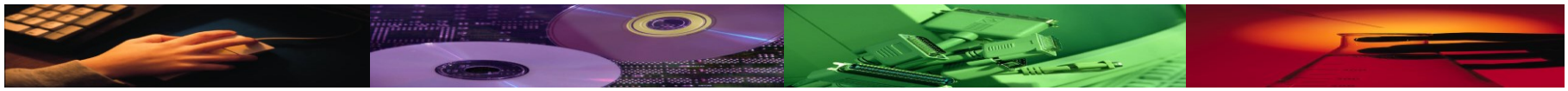
您也可以透過此連結追蹤包裹的進度。
如果您未能在兩日內回覆，此包裹將退回給寄件人。
根據包裹的類型，寄件人將負責退回費用。

您也可以從我們在 106409 臺北市大安區金山南路 2 段 55 號 的倉庫提取包裹。
重新送遞此包裹將收取費用，在上面提供的連結中有詳細說明。

謹致問候
中華郵政

這是一封自動電郵。請不要直接回覆此地址。.

25.測試你的密碼弱不弱



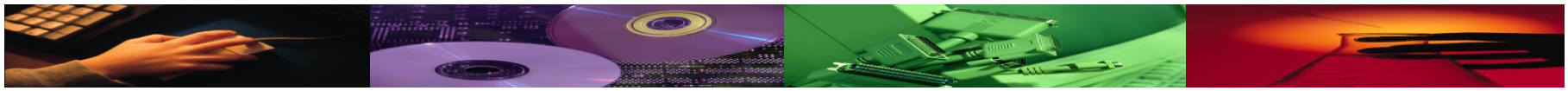
案例解析

- 現今資料洩漏事件頻發，有些人要測試密碼強度是否達到要求，許多駭客藉此心態嘗試蒐集使用者密碼。

安全提示

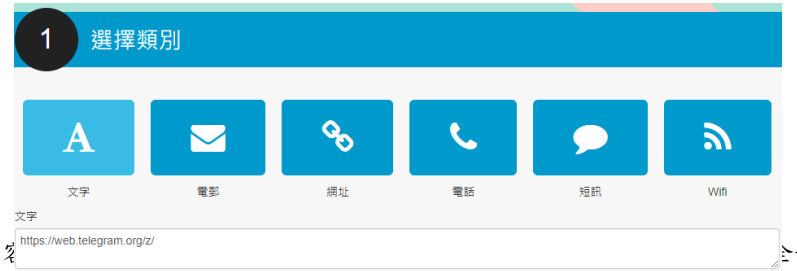
- 最安全的方式是針對每一個網站或系統設置與眾不同的密碼。
- 儘量不要使用測試密碼強度的工具或網站上傳密碼，避免密碼被洩漏。

26.不要亂掃二維碼



案例解析

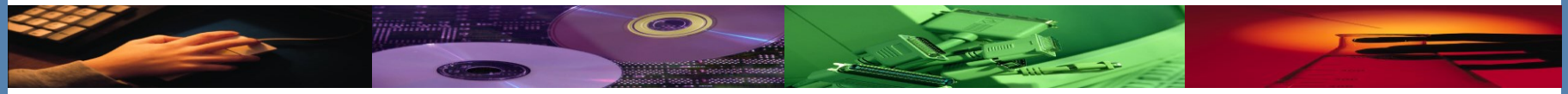
- ✓ 二維碼製作技術門檻低，造成安全隱患。
- ✓ 許多不法份子會把自動下載病毒、垃圾軟體、勒索病毒的鏈接生成二維碼，誘導使用者掃描。



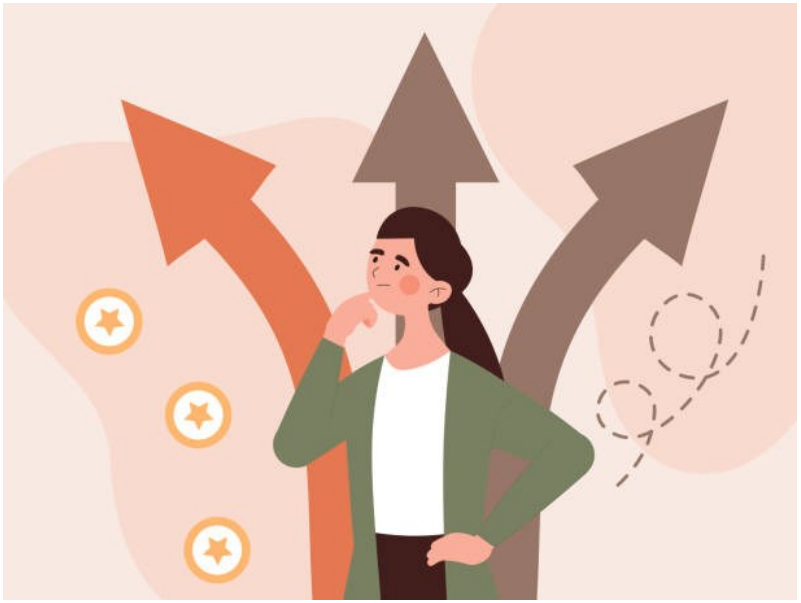
安全提示

- ✓ 來源不明的二維碼不要亂掃，儘量通過官方管道獲取相關二維碼訊息。
- ✓ 掃描後，查看網址是否有異常。
- ✓ 安裝手機防毒軟體，及時阻斷風險。
- ✓ 付款時儘量讓對方掃描付款碼，或與商家確認後再掃描。

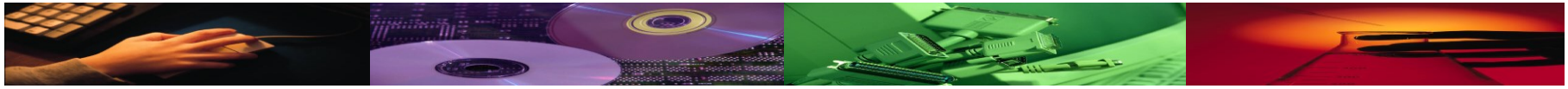
結語



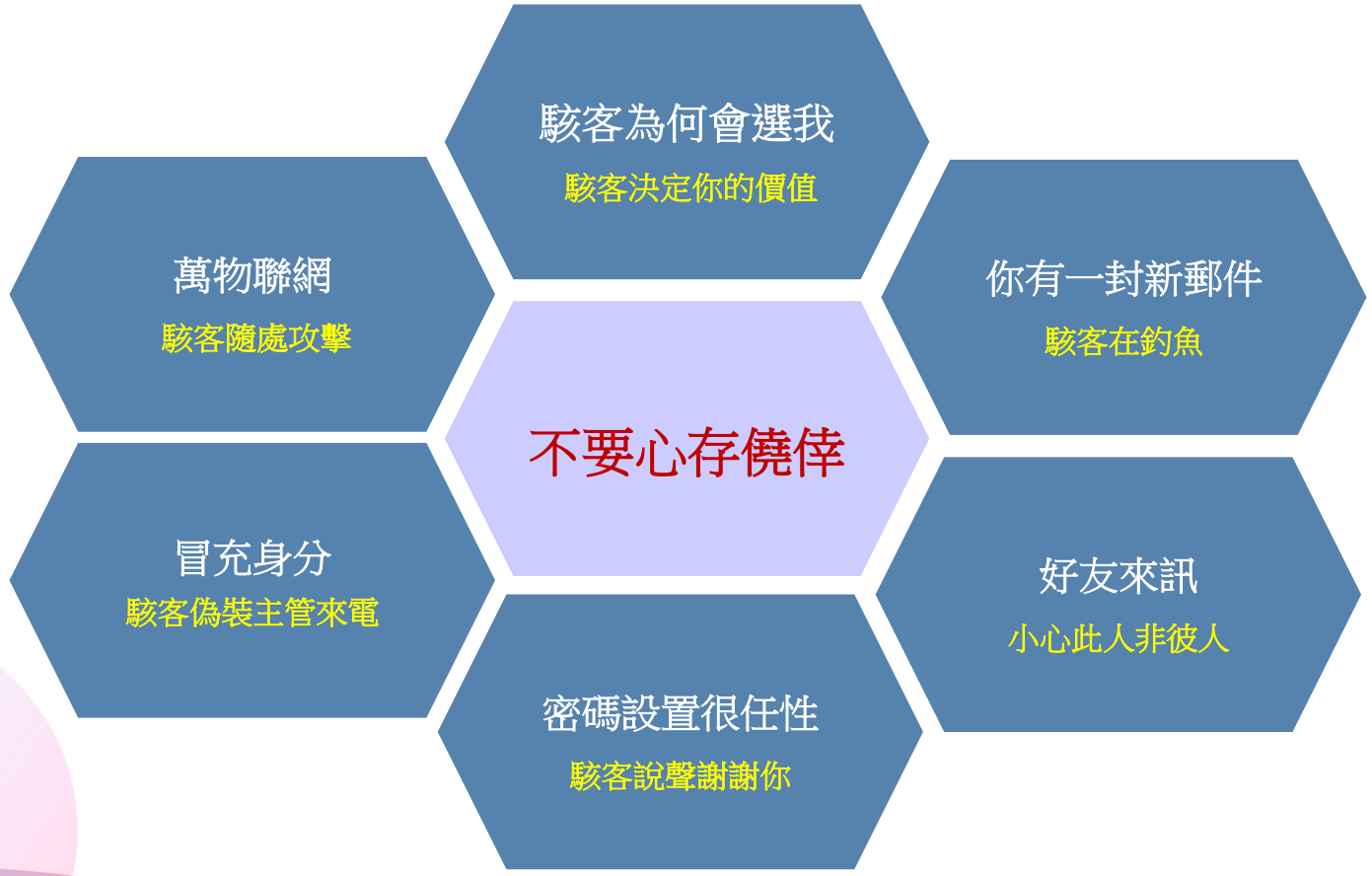
- 一般使用者或員工都是駭客的攻擊目標
- 認清社交工程攻擊
- 防範釣魚郵件
- 防範勒索軟體
- 設置完美密碼就是如此簡單



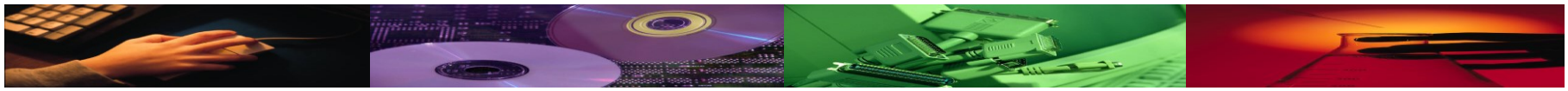
一般使用者或員工都是駭客的攻擊目標



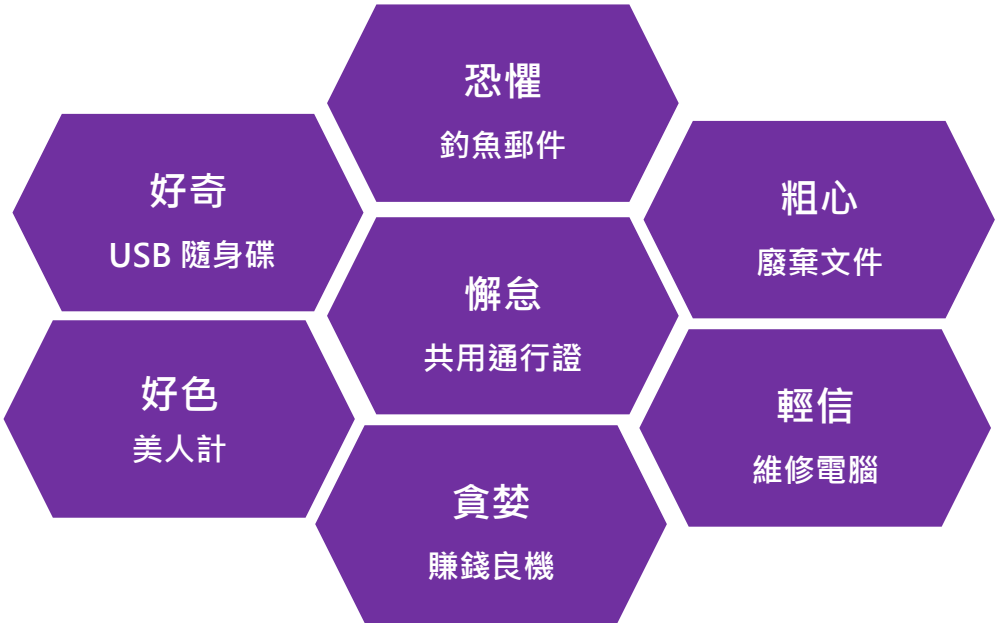
- 四不原則
  - 不輕信
  - 不亂點
  - 不貪心
  - 不好奇



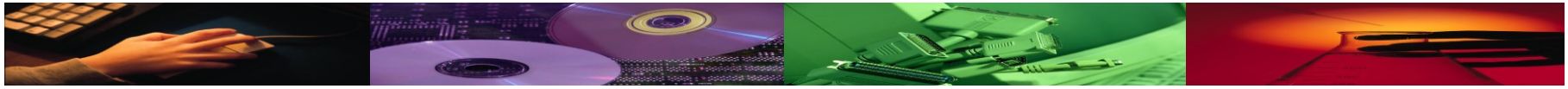
認清社交工程攻擊



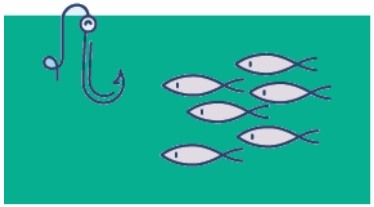
- 社交工程
  - 攻擊者利用人性弱點，誘使你做一些不該做的事情，從而獲取自身利益
- 人性的七大弱點



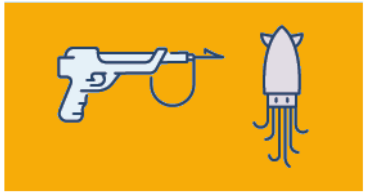
防範釣魚郵件



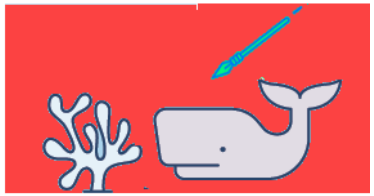
- 釣魚郵件
  - 駭客偽裝成您信任的人，透過電子郵件誘使您回覆郵件、點選鏈結或下載附件
  - 竊取隱私及機敏資訊、詐騙金錢或誘導執行惡意程式
- 網路釣魚分類



一般網路釣魚
Phishing

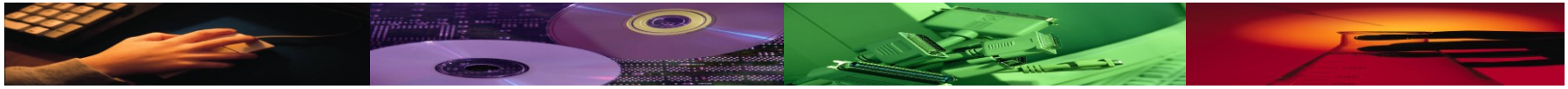


魚叉式網路釣魚
Spear phishing



鯨釣
Whaling

防範勒索軟體

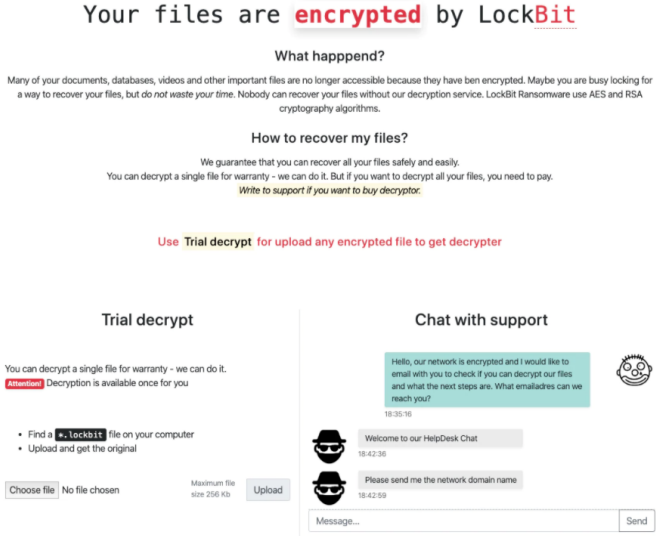


- 勒索軟體
  - 通過惡意程式，加密方式綁架使用者文件或資料，導致使用者無法使用，並以此勒索金錢
  - 就算支付贖金，大部分還是無法打開被加密的文件或資料
- 犯罪手法

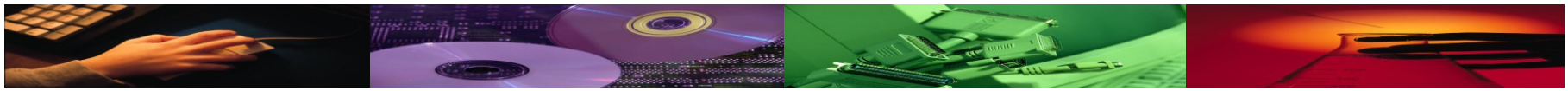
勒索軟體會將系統上的文件、郵件、資料、圖片、壓縮檔案等文件，透過特定形式的加密操作，讓使用者無法使用

通過彈出視窗、對話框或生成勒索通知文件，要求使用者向指定加密貨幣帳戶付款來獲取解密密碼

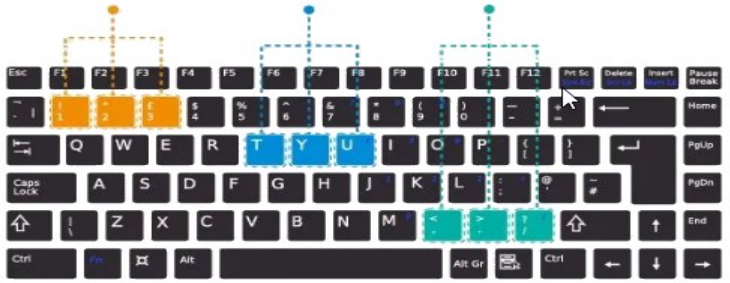
- 預防勒索軟體：一不二要
  - 不點選來源不明的郵件連結、附件
  - 要定期備份重要資料
  - 要安裝防毒軟體，隨時更新



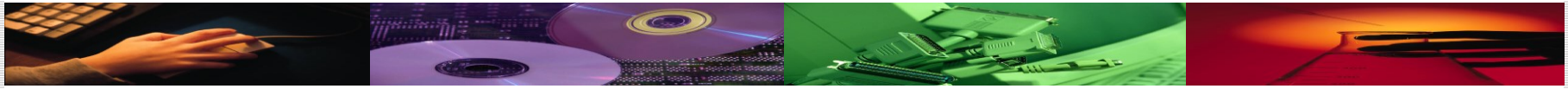
設置完美密碼就是如此簡單



- 完美密碼
  - 安全
  - 好記
- 密碼是怎樣被破解的
  - 如果駭客就是你認識的人
    - 直接用你小孩名字、生日、寵物名字
    - 正確回答找回密碼的問題
  - 如果駭客不是你認識的人
    - 使用最常見的密碼組合
    - 暴力破解密碼
- 設定安全好記的密碼
  - 使用數字、大小寫字母、特殊符號



- 增加密碼長度
  - 暴力破解時間
    - 10個字元(一星期)、15個字元(一世紀)
  - 設置便於記憶的密碼
    - 私立長庚大學 nxu4t;6e/284vm,6



資訊安全
需要大家共同努力~