資安威脅趨勢及案例分享

Agenda

- 前言
- 資安威脅趨勢
- 資安新聞事件
- 破解目標式勒索、無檔案攻擊
- 如何因應與面對
- Q&A

電腦病毒屬於電腦程式的一種，是由**有心人士為了特定的目的**而撰寫出來，再透過各種方式的散佈，依照其病毒程式執行的特性，造成不同的後果，更具體的病毒常見特性：

- 會將本身複製到其他正常檔案或開機區
- 通常同一台電腦內的其他檔案都遭殃
- 不一定具有破壞性
- 危害程度不一
- 發作時間是否固定並無限制

蠕蟲也是病毒的一種，與病毒不同的是「蠕蟲不會感染寄生在其他檔案」。

蠕蟲的主要入侵與繁衍方式為，透過網路連線或電子郵件的附件散播，主要**利用主機的安全弱點進行**，弱點包括了以下幾點:

- 作業系統的弱點
- 應用程式的弱點
- 不安全的權限設定
- 伺服器的弱點
- 使用者不安全的使用習慣

使用薄弱密碼來進行網路檔案共享的電腦很有可能遭受該蠕蟲的感染

個人電腦/伺服器只要完整且即時的的完成更新,搭配嚴謹的密碼原則,隨時保持更新的防毒與安全軟體,以及不採用薄弱密碼的分享將可以避免已知蠕蟲的感染

可攜式設備如USB有可能因為其連接的電腦因為已經被感染而受到影響

個人電腦/伺服器只要開啟分享就有極高的可能被感染

個人電腦/伺服器只要沒有完成更新有極高的可能性會遭受感染

Worm:Win32/Conficker會自動產生網路連線搜尋未完成更新程式安裝,使用薄弱密碼進行分享的儲存空間與檔案以及正在使用可攜式設備如USB的電腦,進行感染

特洛伊木馬 (簡稱 Trojan) 是一種電腦程式，特性如下：

- 偽裝成某種有用或有趣的程式，比如螢幕保護程式、算命程式、影片編碼等
- 包藏禍心，暗地裡做壞事；它可以破壞資料、騙取使用者的密碼等等
- 一般定義上，特洛伊木馬不會自我複製
- 不會主動散播到其他的電腦

間諜軟體會在你不知情或未經過你許可的狀況下，擅自**搜集個人資訊**，再伺機將資料外傳，下載未知的共享程式、免費遊戲或不明來源的其他軟體，都可能讓您受到間諜軟體的威脅。

例如:TSPY_ONLINEGA

透過HTTP與SMTP散播，

當使用者開機、預覽Email

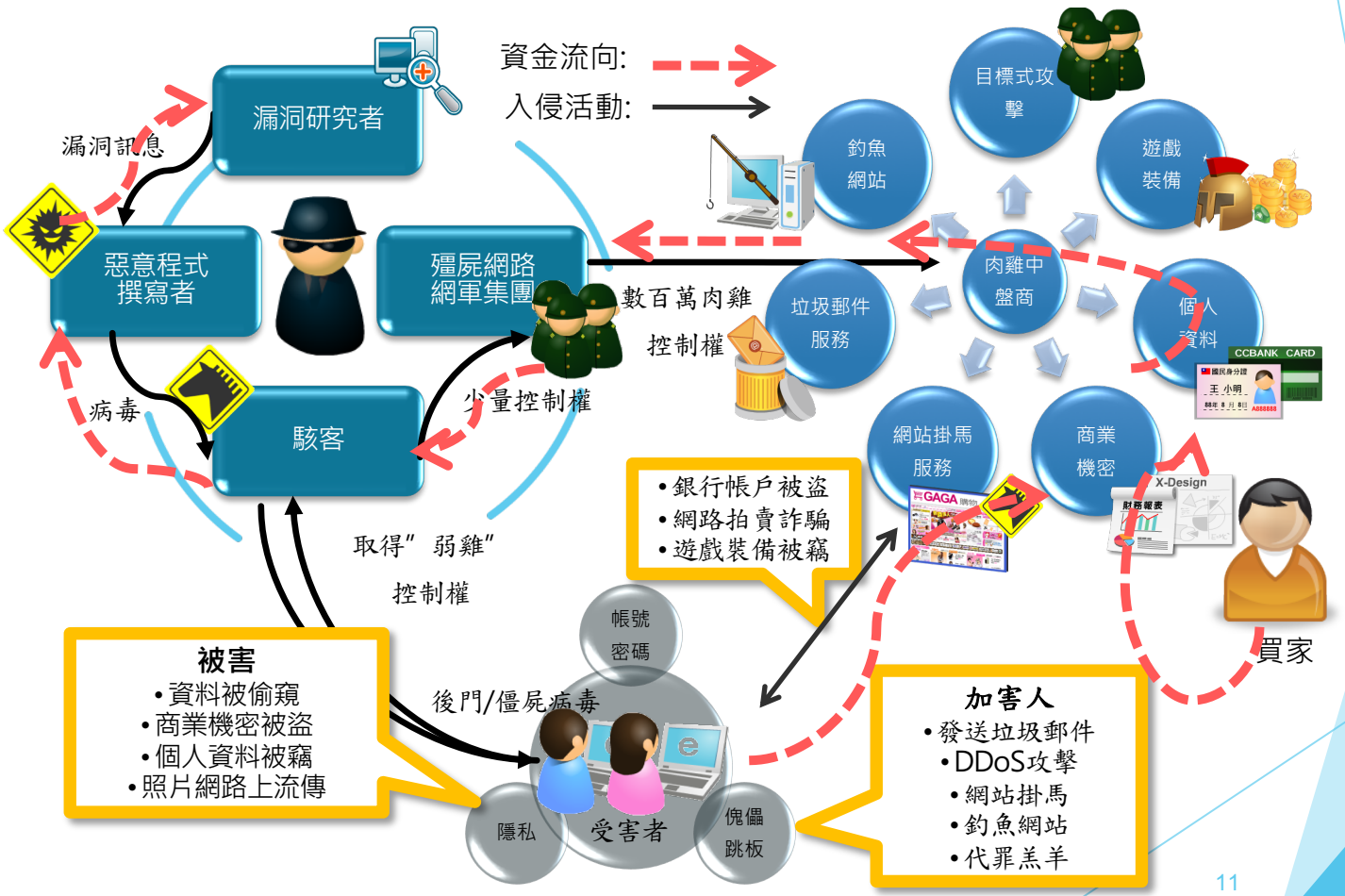
或是訪問惡意網站時此病毒會自動執行，

下載其他病毒、竊取帳號密碼、

以及鍵盤側錄，造成Email Server繁忙、

或是網路流量暴增。

黑色產業鍊


資金流向:
入侵活動:
漏洞研究者
漏洞訊息
惡意程式撰寫者
殭屍網路網軍集團
駭客
病毒
數百萬肉雞控制權
少量控制權
取得"弱雞"控制權
釣魚網站
目標式攻擊
遊戲裝備
垃圾郵件服務
肉雞中盤商
個人資料
網站掛馬服務
商業機密
買家
•銀行帳戶被盜
•網路拍賣詐騙
•遊戲裝備被竊
被害
•資料被偷窺
•商業機密被盜
•個人資料被竊
•照片網路上流傳
帳號
密碼
後門/僵屍病毒
隱私
受害者
傀儡跳板
加害人
•發送垃圾郵件
•DDoS攻擊
•網站掛馬
•釣魚網站
•代罪羔羊

- 不要懷疑單位是否會成為駭客的目標

- 「世界上大型企業分兩種：一種是已經被駭客入侵，另一種則是被入侵卻渾然不知的公司。」

  --- FBI 局長 James Comey

Agenda

- 前言
- 資安威脅趨勢
- 資安新聞事件
- 破解目標式勒索、無檔案攻擊
- 如何因應與面對
- Q&A

資安預測報告各大重點摘要

- 透過**社交工程信的網路釣魚**將取代漏洞攻擊套件成為主要攻擊模式。
- **憑證外洩盜用**事件的數量與嚴重度將大幅提高。
- 員工在家工作及使用家用裝置連網的趨勢，使企業面臨類似**BYOD自帶設備**的資安風險。

網路釣魚案例

在2019年將大幅增加，成為網路犯罪者的主要攻擊管道

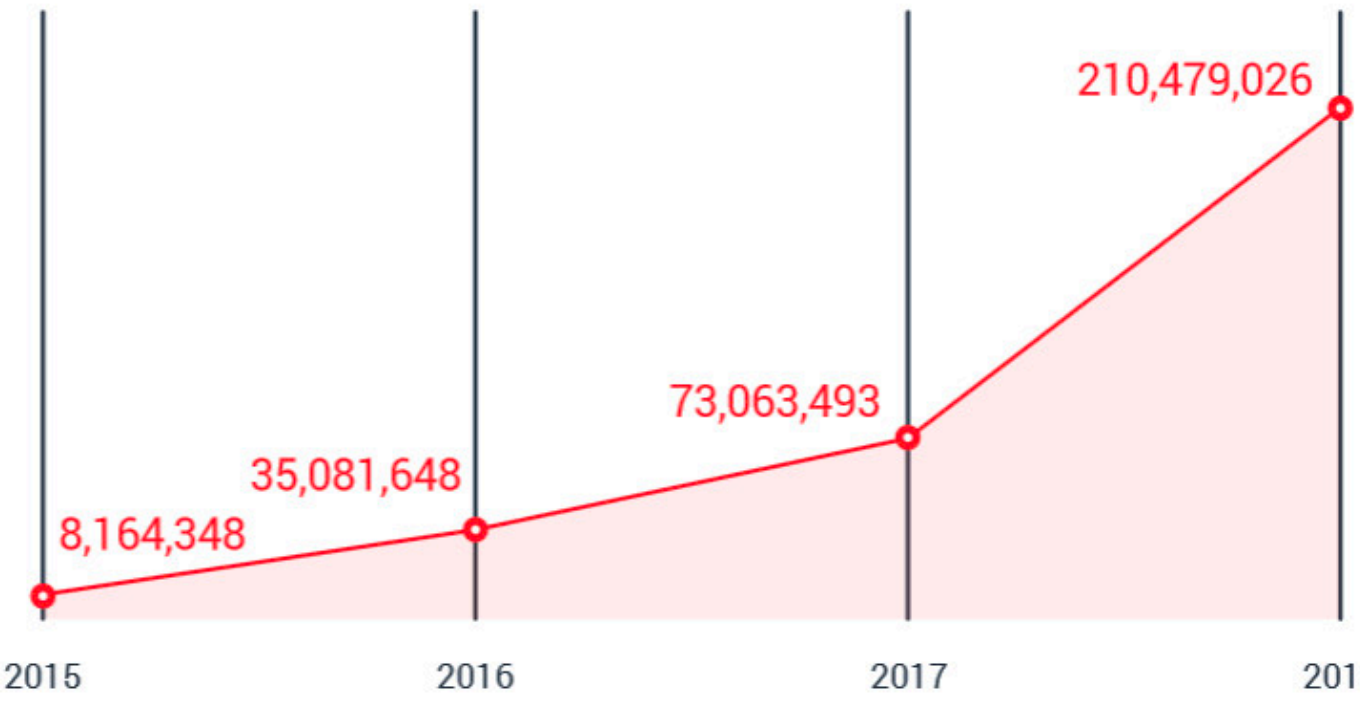


圖 2：已攔截的網路釣魚相關網址數量逐年攀升 (根據趨勢科技 Smart Protection Network 全球威脅情報網 2018 年第三季的統計資料)。

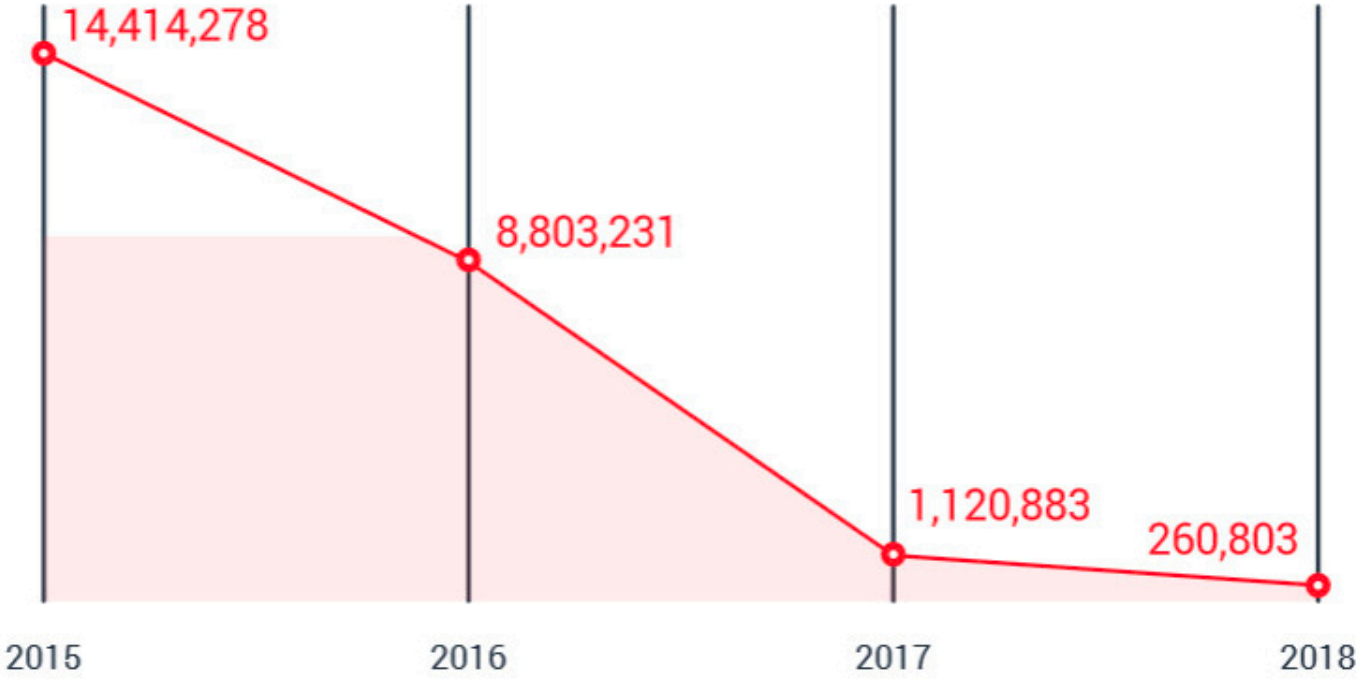


圖 1：已攔截的漏洞攻擊套件活動逐年減少 (根據趨勢科技 Smart Protection Network™ 全球威脅情報網 2018 年第三季的統計資料)。

資安預測報告各大重點摘要

- 歐盟將針對違反GDPR的大型企業開處全球營業額4%或是2千萬歐元高額罰鍰。
- 除了企業管理階層，**變臉詐騙**將更深入企業其他管理層級或是相關員工。
- 自動化將提高商業流程入侵的風險。
- 工控系統的目標攻擊持續成為隱憂，HMI人機界面也將持續成為SCADA監控與資料擷取系統的主要漏洞。

Business Email Compromise

- 網路犯罪手法已由間接誘騙使用者的帳號密碼，轉向直接勒索錢財的「數位勒索」為主，駭客利用勒索病毒威脅受害者付錢贖回資料或透過**變臉詐騙攻擊或稱為商務電子郵件入侵（Business Email Compromise，簡稱 BEC）**手法進行商業詐騙，以獲得高利潤報酬。

Business Email Compromise

※ 專門針對那些經常需要
匯款給外部供應商的企業機構

偽冒報價單及匯款帳戶騙
取客戶匯款

拋棄式郵件信箱

客戶接收駭客通知
匯款被騙

業務郵件遭鎖定

買家

出口商

預防BEC詐騙，從郵件安全做起

A. 養成安全的郵件使用習慣
   a) 不要用免費信箱與共用帳號
   b) 做好基本密碼安全與端點防護
   c) 培養員工資訊安全意識
B. 透過郵件安全產品的進階防護功能，加強企業本身的資安保護
   a) 應用郵件加密方式確保內容安全
   b) 發送BEC測試信，提升員工資安意識
   c) 可啟用專屬的BEC防護功能
   d) 自行設定郵件管控原則
   e) 強化郵件帳號登入安全
   f) 採用郵件身分驗證等機制
C. 強化企業匯款確認流程

Agenda

- 前言
- 資安威脅趨勢
- 資安新聞事件
- 破解目標式勒索、無檔案攻擊
- 如何因應與面對
- Q&A

撞庫攻擊手法

- 帳戶資料外洩，遭盜用詐騙事件將不斷增加
- 不少使用者習慣在不同網站上，**使用相同的帳號密碼**
- 利用大量外流的電子郵件地址和密碼，並透過自動化的方式來嘗試入侵
- 網路犯罪集團藉由入侵網路紅人的社群媒體帳號，藉此執行水坑式攻擊，藉由追隨者的管道以及粉絲信任的心理，散布惡意程式

漏洞資訊

發佈日期	標題
2019-08-02	SanDisk SSD Dashboard 管理程式存有資安漏洞
2019-08-01	Google 資安團隊 Project Zero 一口氣發現多個 iOS 安全漏洞
2019-07-31	微軟 Excel 存有遠端執行任意程式碼漏洞
2019-07-22	Windows Defender Application Control 安控機制可被跳過的漏洞
2019-07-09	羅技等品牌無線鍵鼠 USB 接收器，存有多個嚴重資安漏洞，可能遭劫持
2019-05-31	京晨科技(NUUO Inc.)網路監控錄影系統(Network Video Recorder, NVR)存在安全漏洞，允許攻擊者遠端執行系統指令，請儘速確認並進行韌體版本升級
2019-05-15	微軟Windows遠端桌面服務存在安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

https://twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?id=84

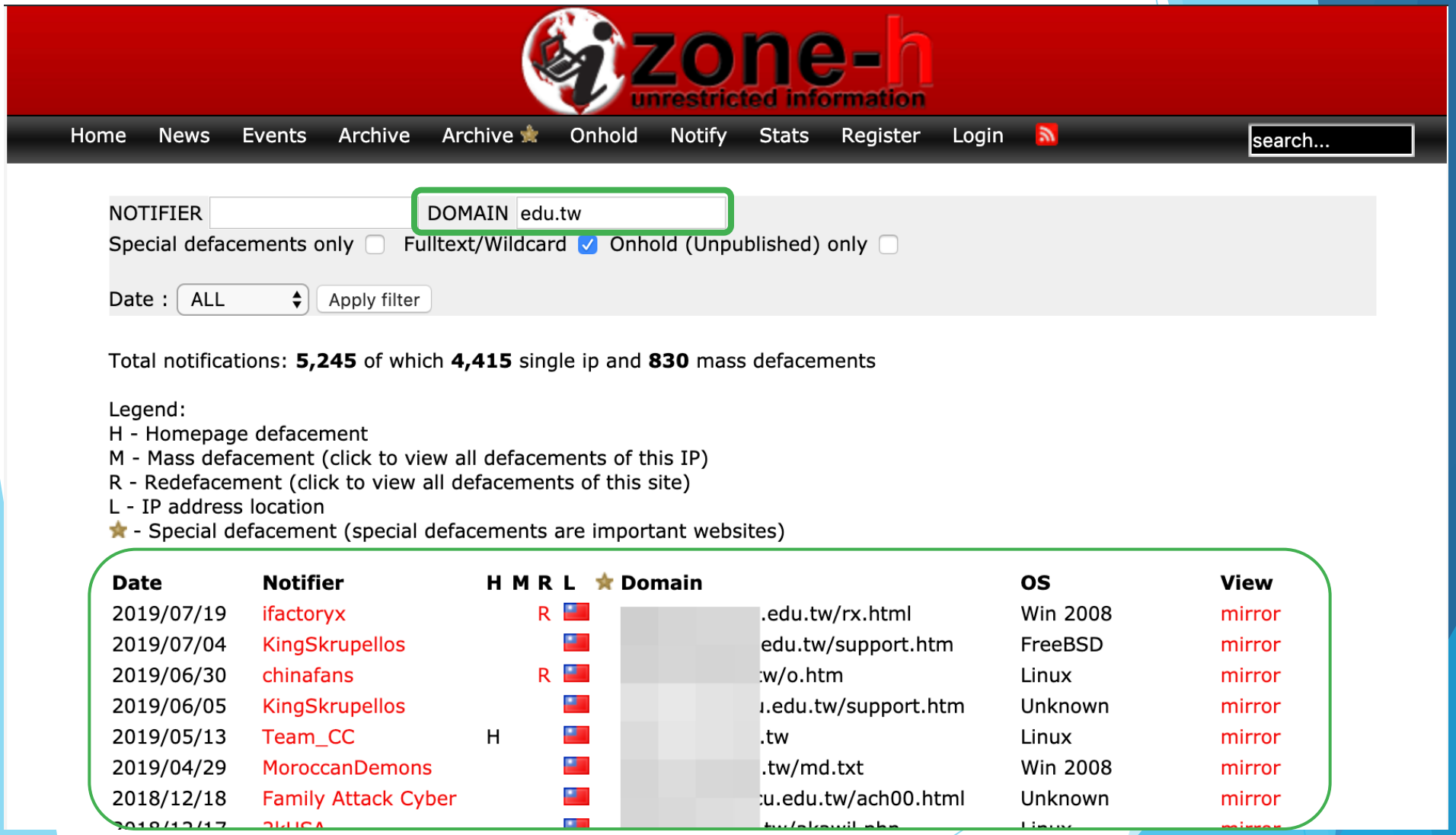
資料外洩事件連環爆,帳密被竊之後...

一旦駭客拿到你帳號密碼，可能發生的七件事

1) 到地下市場兜售
2) 使用線上服務,你買單
3) 進行非法交易
4) 藉以進入企業網路
5) 一組帳密被盜,其他帳密連鎖失守
6) 發動網路攻擊
7) 勒索被駭人

保護帳號小秘訣

A. 點擊連結前,滑鼠先 hold 一下
B. 保持更新
C. 使用*雙因子*認證
D. 定期檢查你的對帳單
E. 在不同的網站使用不同的密碼
F. 不同用途使用不同的電子郵件信箱
G. 取得完整的保護

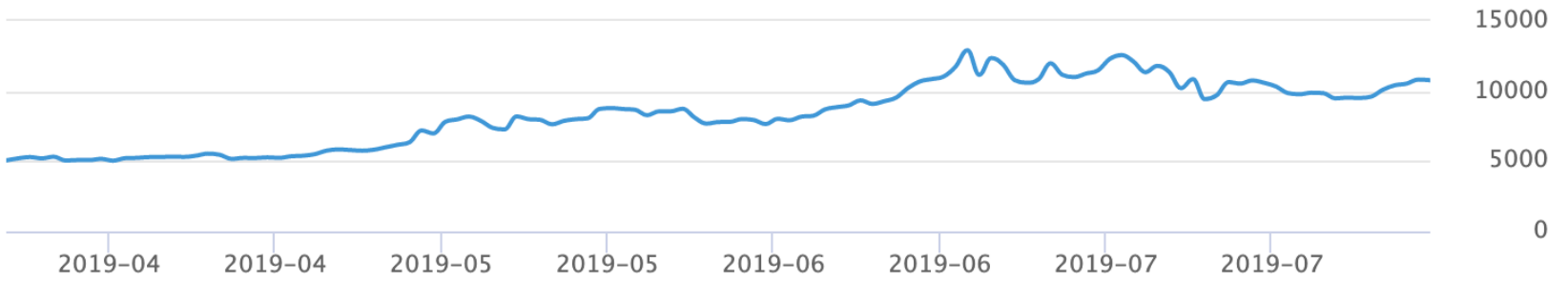


http://www.zone-h.org

比特幣 (BTC)

10,759.61

(24h)
-44.19 | -0.41%



24h | 3個月 | 1年 | 3年

↑	10,922.49 最高價 (24h)	↓	10,538 最低價 (24h)
$	28.94億 成交量 (USD)	$	1,932.56億 市值 (USD)
₿	2,100.00萬 總量 (BTC)	₿	1,785.61萬 產量 (BTC)

緩解措施

- 保持系統及應用程式更新，並考慮使用虛擬修補技術，尤其是老舊的系統和網路。
- 積極監控網路；防火牆和部署入侵偵測和防禦系統可以提供多層次安全防護來對抗惡意威脅。
- 實施最低權限原則：限制或停用可作為進入點的不必要或過期的應用程式和元件。
- 透過部署安全機制（如應用程式控制和行為監控）來實施縱深防禦，防止未經授權或惡意應用程式或程序執行。

Agenda

- 前言
- 資安威脅趨勢
- 資安新聞事件
- 破解目標式勒索、無檔案攻擊
- 如何因應與面對
- Q&A

三個勒索病毒在未來數年仍將持續肆虐的理由

1）勒索病毒持續進化中

- 大多數的勒索病毒都屬於檔案加密型或上鎖型
- 另一種的上鎖型勒索病毒則是會鎖住中毒設備的作業系統

2）勒索病毒對駭客來說是個金雞母

- 駭客不需要經過中間人就可以直接獲取金錢回報
- 勒索病毒的威脅無處不在，而且某些產業會更被針對。

3）不缺乏目標: 從個人用戶到大企業都會被攻擊

- 資料的重要性以及依賴資料來進行日常運作，讓某些產業更加容易遭受勒索病毒。這包括：
  - 醫療機構
  - 政府機構
  - 教育機構
  - 法律事務所

Agenda

- 前言
- 資安威脅趨勢
- 資安新聞事件
- 破解目標式勒索、無檔案攻擊
- 如何因應與面對
- Q&A

面對 接受 處理

打的愈深、挖的愈多

- 當防火牆規則設計不當
- 行動辦公服務遭到惡意利用
- 利用網頁後門，達到內網滲透
- 百密可能一疏

為何駭客能一再突破

① 主機存在漏洞

② 關鍵主機缺乏保護

③ 可輕易取得密碼

④ 遠端程式任意使用

⑤ 網路區隔設計不佳

⑥ 缺乏威脅監控機制

網路區隔設計不佳

a) 在內網可任意RDP、Psexec
b) 外網可對內網進行RDP
c) 重要主機可任意存取外部網路
d) 測試主機可直接對外網訪問
e) VPN連線至內網，限制不足
f) 主機群沒有分級管理
g) …

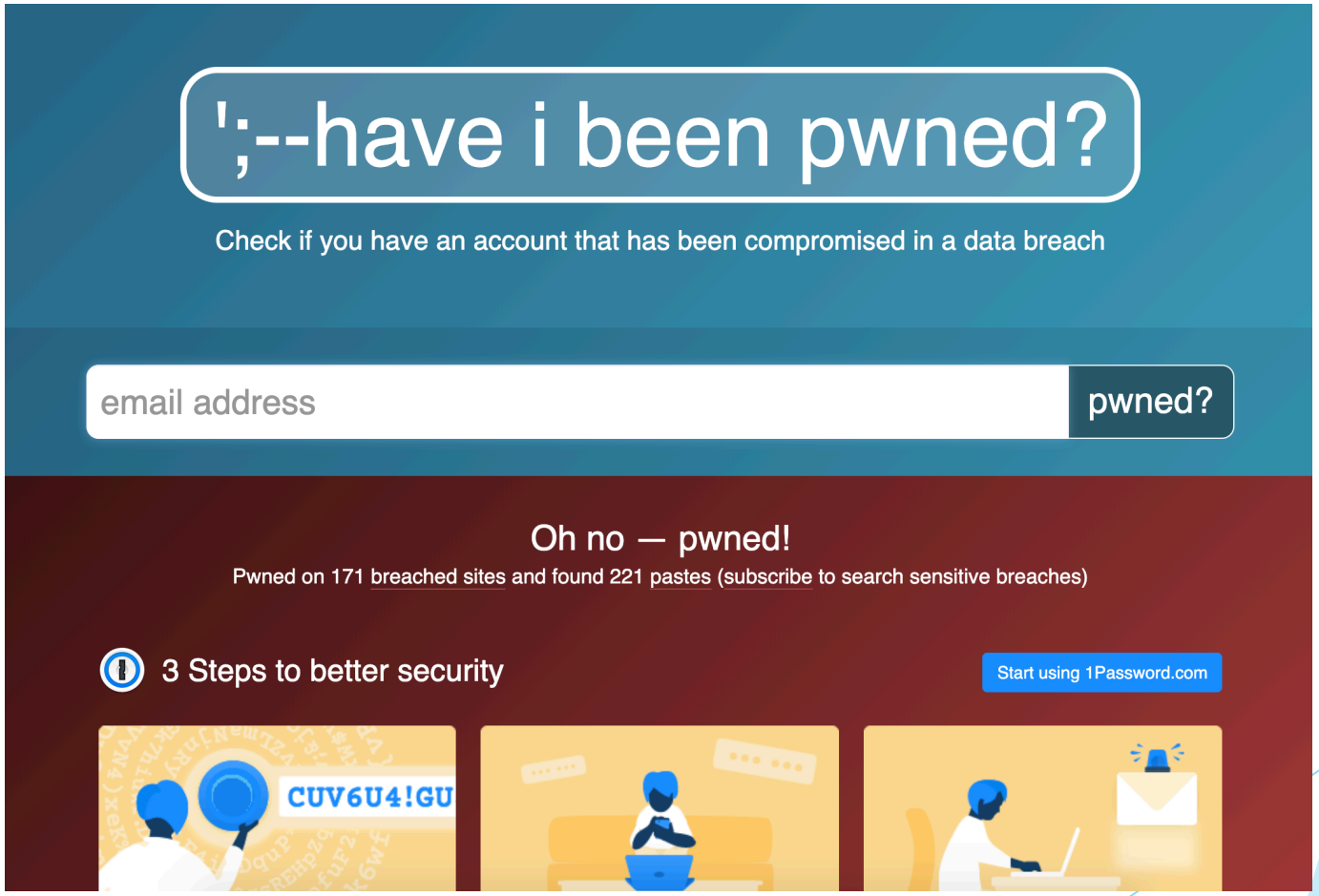
零信任模式勢在必行

Never Trust, Always Verify

缺乏威脅監控機制

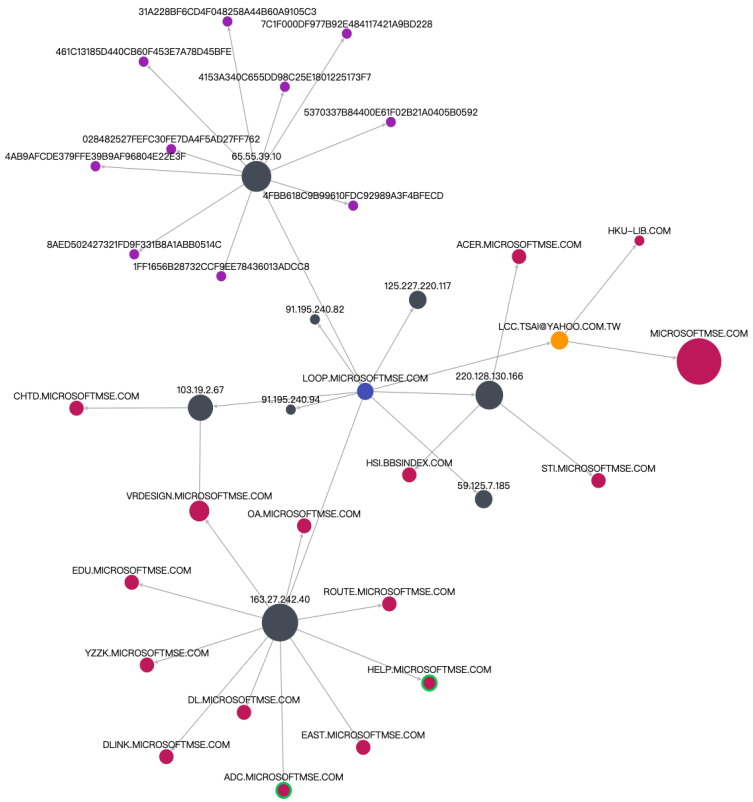
- 主機異常行為監控
  - 帳號的異動
  - 檔案的異動
  - 系統設定的異動
  - CPU、磁碟、記憶體等使用率的異常變化
  - LOG異常清除
- 內部網路異常流量監控
  - 檔案傳輸
  - 遠端指令或排程
  - 針對性能問題影響業務的流量監控

查詢自己的帳密是否被曝光



https://haveibeenpwned.com/

HELP RSS API FEED MALTEGO CONTACT SEARCH



DOMAIN > LOOP.MICROSOFTMSE.COM

Welcome! Right click nodes and scroll the mouse to navigate the graph.

More information on this domain is in **AlienVault OTX**

IS THIS MALICIOUS?

Yes | No

WHOIS

Property	Value
Email	lcc.tsai@yahoo.com.tw
NameServer	NS2BLS.DOMAINSITE.COM
Created	2012-05-14 00:00:00
Changed	2015-05-07 00:00:00
Expires	2016-05-14 00:00:00
Registrar	DOMAINSITE, INC.

DNS RESOLUTIONS

https://www.threatcrowd.org/

釣魚演練平台

TREND MICRO PHISH INSIGHT 首頁 模擬演練 教育訓練 服務方案 登入 註冊

進行釣魚模擬演練，免費！提升員工資安意識，無價！

Starter

$免費

20 個收件人 / 任務
1 個寄送網域

您不需做額外的設定，即可建立演練任務，發送模擬的網絡釣魚郵件給指定的收件人。但是**限制收件人必須與您的帳戶是相同的電子郵件網域**，且一個任務最多只能寄給 20 個收件人。

例如，我註冊的帳戶是 admin@abc.com，我可以寄信給 user1@abc.com，但是無法給 user2@xyz.com。

此方案適用於 DNS 伺服器是由網域代管商管理的組織。

Popular

Standard

$免費

200 個收件人 / 任務
無限個寄送網域

將 TXT 機碼新增到您帳戶網域的 DNS 伺服器，您就會升級到 Standard。

之後您即享有發送網絡釣魚郵件給至多 200 個收件人的權利，如果您的組織有多個電子郵件網域，請將 TXT 機碼新增到這些網域，您也可以發送電子郵件給這些網域的收件人。

這是 Phish Insight 的一項安全機制，以避免用戶對不相關的人寄送垃圾郵件。

Premium

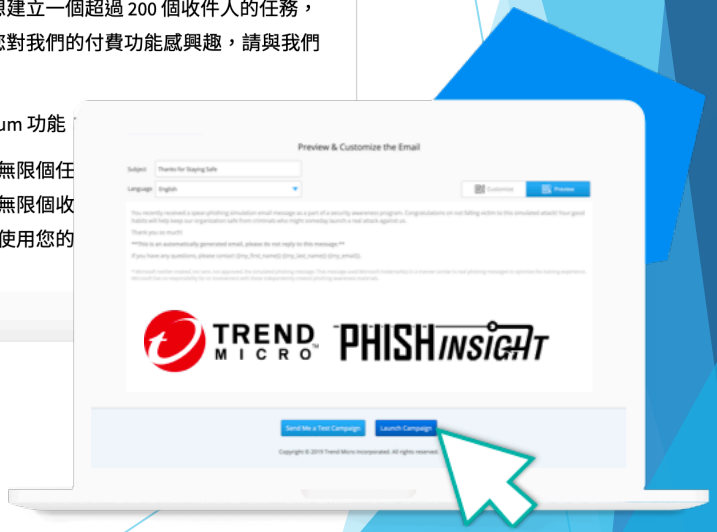
聯絡我們

無限個收件人 / 任務
無限個寄送網域

若您想建立一個超過 200 個收件人的任務，或者您對我們的付費功能感興趣，請與我們聯繫。

Premium 功能

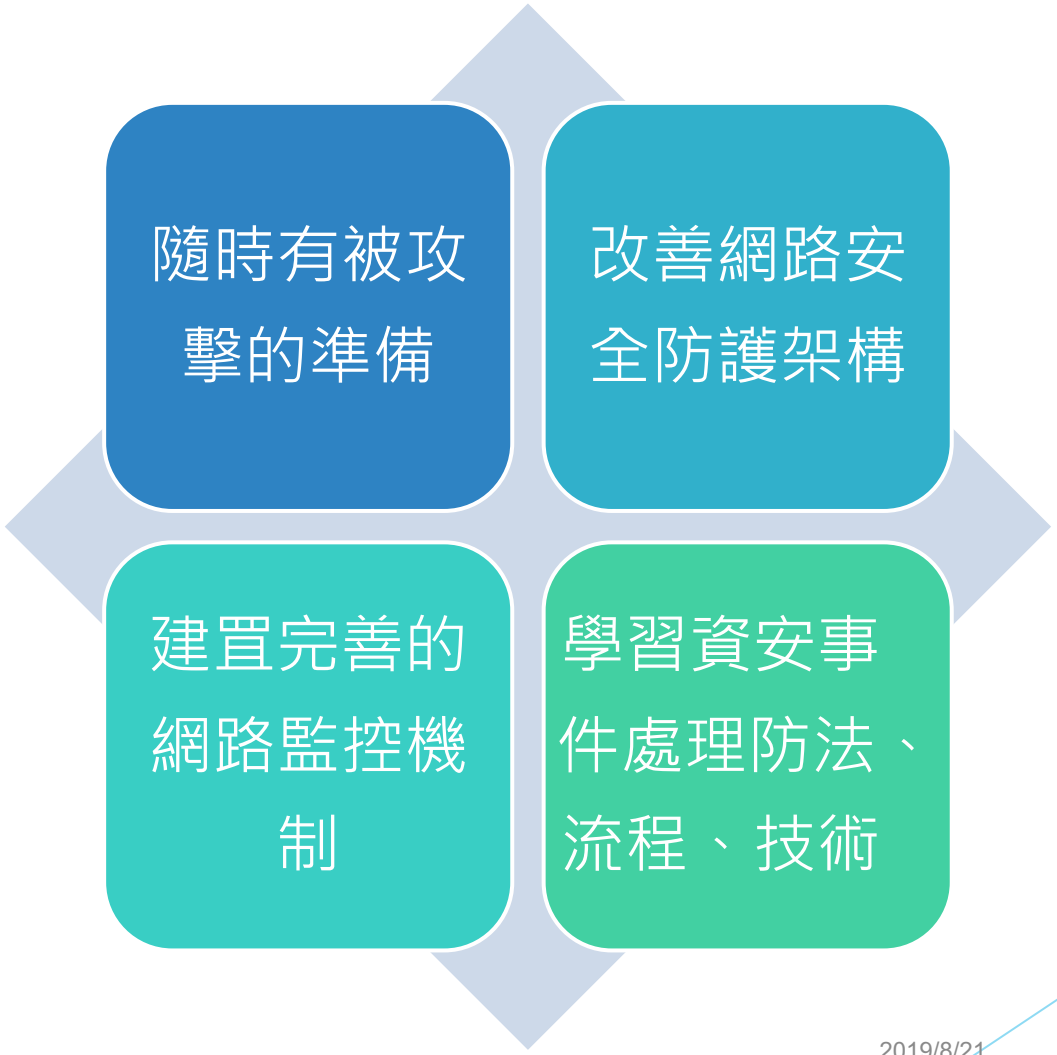
- 無限個任
- 無限個收
- 使用您的



https://phishinsight.trendmicro.com/zh-tw/

Agenda

- 前言
- 資安威脅趨勢
- 資安新聞事件
- 破解目標式勒索、無檔案攻擊
- 如何因應與面對
- Q&A


隨時有被攻擊的準備
改善網路安全防護架構
建置完善的網路監控機制
學習資安事件處理防法、流程、技術

面對加密勒索軟體，你該知道的防護策略大揭露

勒索軟體因應對策

階段	事前預防	即時處置	事後宣導
作法	●定期更新軟體	●斷網關機	●事件分析
	●只打開信任的郵件	●清查受損範圍	●人員教育
	●安全防護軟體	●資料復原	●權限管控
	●定期備份檔案		●強化防護

資料來源：趨勢提供，iThome 整理，2016 年 7 月

給企業/單位的建議

- 重設管理員帳號密碼，增加密碼強度（長度與複雜度）
- 重新檢視並設定使用者權限，不讓單一帳號擁有過大的權限； IT人員時常使用許多工具與服務，但這些工具也可被駭客用於非法行為，在案例中就是PsExec，因此必須設定權限加以控管；
- 勒索病毒攻擊手法日新月異防不勝防，務必以三二一原則妥善備份重要檔案（三份備份，分別存放在兩種不同類型的裝置，一份放在異地或安全地點）；
- 務必保持更新系統與網路，降低安全性漏洞遭到入侵的機率。如原廠尚未釋出修補程式，也可利用虛擬補丁進行防護；
- 加強資安教育訓練，讓員工了解公司的資安政策，並加強員工的資訊安全觀念；
- 部署多層次資安防護機制解決方案，除了端點防護解決方案以外，進階沙箱分析隔離不明檔案，應用程式控管與行為監控則可防止可以檔案執行，並避免系統遭到未經授權的變更；
- 利用設備過濾網路中可疑的APT攻擊活動
- 重新檢視並整理例外清單

~ Thank You ~