資安認知宣導教育訓練-

勒索病毒之威脅與防護

國際登錄核可 ISO27001/BS10012/ISO9001主導稽核員

國際登錄核可 FSSC 22000 / ISO 22000主導稽核員

TPIPAS 個人資料保護管理師 / TPIPAS 個人資料保護驗證師

Mobile: 0935701552

E-mail: arvin.fang@msa.hinet.net

博創資訊科技

資深顧問師

方煥文

課程大綱

Course Outline

- 近期資安事件情資分享
- 認識勒索病毒
- 勒索軟體安全防護
- 結語

近期資安事件情資分享：臉書瘋傳假 Youtube連結

- 2022年7月19日，如果你的朋友用臉書私訊你,還附上一個來自"即時新聞"社團的影片連結,問:「這是你嗎？」你會不會不假思索的點入連結,看看自己是不是成了醜聞中的主角?

- 這就是流傳一陣子,讓許多人卸下心防的臉書網路釣魚手法。近日有了新變種:「我覺得他長得像你」、「看看我發現了什麼？」,這次除了竊個資,還會故佈疑陣,跳出手機中毒警告訊息,引導你移除病毒,其實是背地裡安裝不明 app,還要跟你收費。

近期資安事件情資分享：「思科被駭」

2022年8月17日，雲端通訊平台Twilio和網路巨頭思科（CISCO）先後遭遇駭客社交工程攻擊並發生資料洩露，兩家公司的員工成了駭客的突破口，這再次凸顯了人員依然是當今網路安全最難以修補的「漏洞」。

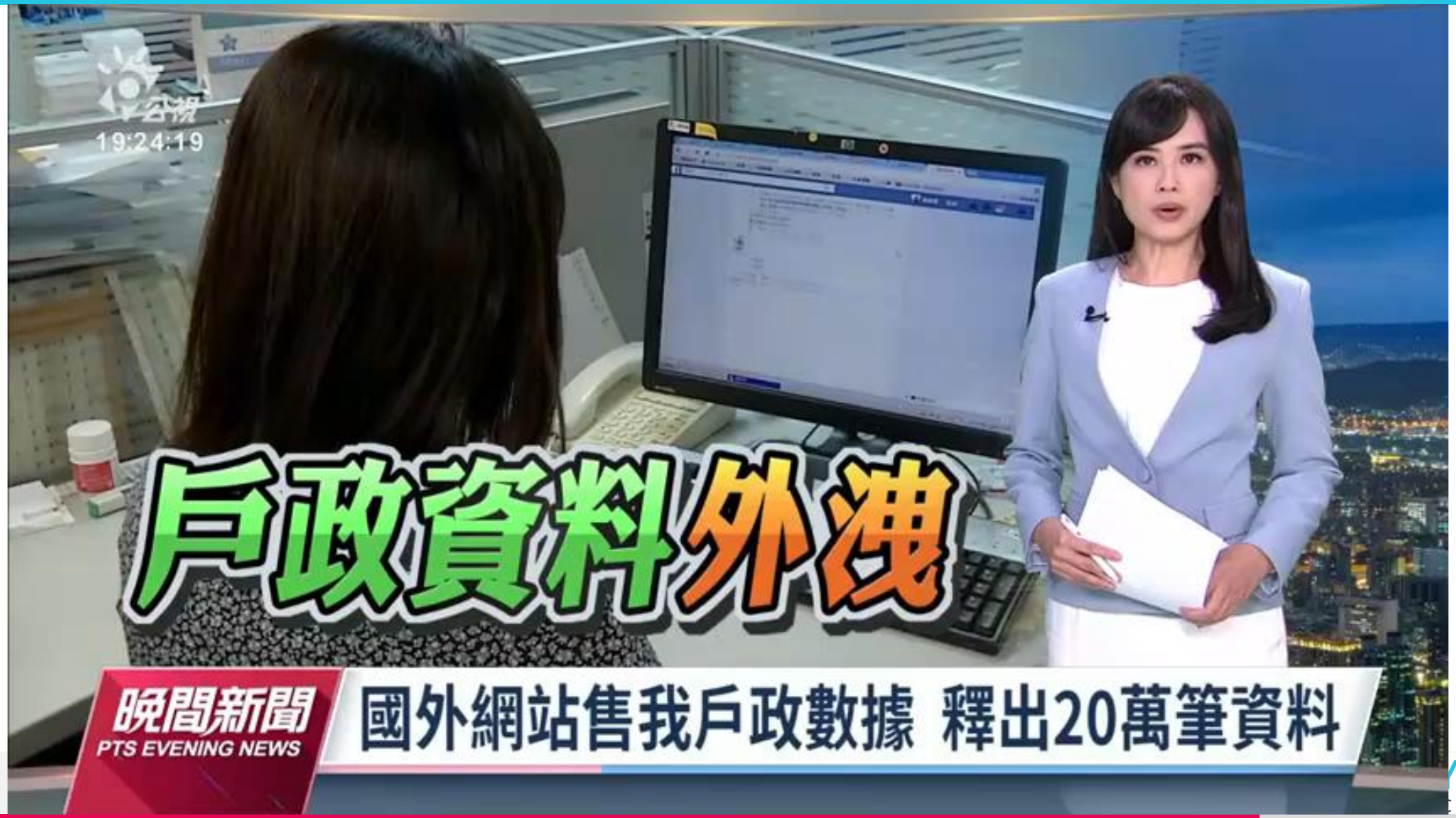
Twilo和思科的資料洩露事件都表明，企業不能僅依靠員工來識別日益複雜的社交工程騙局，即使是這些員工本身也是IT技術人員。

近期資安事件情資分享：Uber 疑遭駭客入侵內部系統

共享乘車與送餐服務大型業者 Uber，於本（2022）年 9 月 15 日發布資安通報，指出該公司發生內部系統遭駭侵者以社交工程攻擊手法入侵的資安事件；據紐約時報指出，這次攻擊事件可能肇因於某位員工遭到一名年僅 18 歲的駭侵者，透過社交攻擊手法取得該公司內部系統的登入資訊。

各組織應加強員工資安宣導，防範員工成為社交攻擊破口；內部系統的重要存取密碼也需善加保護，以免遭駭侵者輕易取得，用於發動進一步攻擊。

近期資安事件情資分享：個資外洩案例1



近期資安事件情資分享：個資外洩案例1

問題分析	**若為政府機關流出，則應檢視戶政單位之資安/個資管理系統運作之狀況；若為政府機關委外單位(即民間企業)流出，則須檢視政府機關是否做到「個人資料保護法施行細則第8條」之相關委外監督之管理。**
防範方式	1. 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 A. 配置管理之人員及相當資源。 B. 界定個人資料之範圍。 C. 個人資料之風險評估及管理機制。 D. 事故之預防、通報及應變機制。 E. 個人資料蒐集、處理及利用之內部管理程序。 F. 資料安全管理及人員管理。 G. 認知宣導及教育訓練。 H. 設備安全管理。

近期資安事件情資分享：個資外洩案例1

發生時間	2022/10/30
事件概述	台灣戶政系統疑似遭駭客入侵，有網友日前在國外論壇說要賣來自台灣戶政網站的數據，並先釋出約20萬筆個資。初步調查這20萬筆主要集中在宜蘭，連縣長林姿妙等人個資都在其中。內政部否認數據由戶政系統流出，但資安專家推測，可能是戶政系統與其他系統串接時有漏洞才導致外洩。

近期資安事件情資分享：個資外洩案例1

防範方式	I. 資料安全稽核機制。 J. 使用紀錄、軌跡資料及證據保存。 K. 個人資料安全維護之整體持續改善。 2. 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。
衝擊影響&省思	1. 個資外洩事件的頻傳，儼然以對民眾隱私權衝擊造成甚大影響，進而造成詐騙事件屢屢增加，這些皆是政府機關、民間企業仍須努力改進的地方。 **2. 須謹慎追究資料流出之方式，進而採取相關防護措施。**

近期資安事件情資分享：個資外洩案例2

近期資安事件情資分享：個資外洩案例2

發生時間	2021/05/13
事件概述	新冠肺炎疫情趨緩，新北市運動中心才解封不到10天，就被爆出實名制資料外洩情形，網友在ptt發文表示，**新北市運動中心保存的個資，不但可以在網路上公開瀏覽，甚至還能刪除、修改內容，完全沒設任何權限**，讓網友看傻眼，甚至還有人惡搞，在表單上貼罷韓文宣，對此新北市體育處回應，初步調查是**被駭客入侵**。
問題分析	此運動中心因使用Google表單蒐集個資，對蒐集之個資檢視修改等權限未適當把控，引起駭客惡意入侵。
防範方式	1. 不使用網路共享雲端蒐集/處理/利用太過敏感之個資檔案。 2. 若使用雲端傳輸檔案，應對檔案進行適當**加密**，以免個資外流。
資料來源	https://www.youtube.com/watch?v=BBBb9qa8oLA

近期資安事件情資分享：個資外洩案例3

近期資安事件情資分享：個資外洩案例3

發生時間	2022/02/10
事件概述	台南市警局，去年9月在內部稽查時發現，歸仁分局交通分隊一名員警，利用職務之便，調閱大量民眾個資，非法提供給當鋪業者，每筆收3千到1萬元不等，不當獲利約2萬5千元。檢方偵訊後，當鋪業者和員警被收押禁見，記兩大過，警察的工作也丟了。
問題分析	員警對於個資保護及法治觀念不足，依此案例非但違反個人資料保護法，並違反貪汙治罪條例。
防範方式	1. 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 2. 認知宣導及教育訓練。 3. 存取權限控制與使用者操作軌跡。
資料來源	https://www.youtube.com

近期資安事件情資分享：個資外洩案例4

近期資安事件情資分享：個資外洩案例4

發生時間	2022/10/20
事件概述	台北市刑大，傳出風紀案件！日前新北地檢署，偵辦一起詐欺「水房案」，發現，北市刑大偵五隊的1名楊姓偵查佐，與從事詐騙集團的戴姓女子交往。疑似利用職權，查閱警用電腦系統，提供民眾個資給對方，還會回報警方追查進度，涉嫌、收賄，數百萬元。
問題分析	員警對於個資保護及法治觀念不足，依此案例非但違反個人資料保護法，並違反貪污罪、組織犯罪、加重詐欺、洗錢等罪嫌。
防範方式	1. 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 2. 認知宣導及教育訓練。 3. 存取權限控制與使用者操作軌跡。
資料來源	https://www.youtube.com

近期資安事件情資分享：個資外洩案例5

近期資安事件情資分享：個資外洩案例5

發生時間	2022/07/10
事件概述	台南市華平派出所一名警員，6月下旬利用警政電腦系統查詢職棒啦啦隊女孩們的個資，市警察局發覺查核異常，調查他非因公使用電腦，對他記2支小過，並停止查詢系統權限。派出所所長督導不周，連帶處分申誡一支。
問題分析	員警對於個資保護及法治觀念不足，依此案例該員警之行為已違反個資法15條之規定：非法定職務必要範圍、未經當事人同意且侵害當事人權益。
防範方式	1. 公務機關保有個人資料檔案者，應指定專人辦理安全維護事項防止個人資料被竊取、竄改、毀損、滅失或洩漏。 2. 認知宣導及教育訓練。 3. 存取權限控制與使用者操作軌跡。
資料來源	https://www.youtube.com

認識勒索病毒

Introduction to Ransomware

認識勒索病毒 – 影片觀賞


FBI也沒轍
勒索軟體迷網全球!
我們國內現在很糟糕的
FBI也沒轍 勒索軟體迷"網"術入侵台灣!
17672.90
32.45
外資買 09 華南金 5296張 10 台灣50 4622張

認識勒索病毒

勒索軟體：

- 又名流氓軟體
- 起源於俄羅斯
- 可將使用者的電腦鎖住
- 亦可將使用者的所有檔案加密
- 並且在電腦中留下聯繫方式，要求受害者交付贖金，才能取得將檔案解密的解密金鑰
- 獲得贖金是這類病毒的最終目標

認識勒索病毒

- 加密性勒索軟體
  - 最早已知的此種病毒是1989年的“AIDS” Trojan病毒。
  - 該病毒的實體數據會宣稱受害者的某個軟體已經結束了授權使用，並且加密磁碟上的檔案，要求繳出189美元的費用給PC Cyborg Corporation以解除鎖定。
  - 在2006年中，勒索軟體開始運用更加複雜的RSA加密手段
  - 2008年6月，發現了新變種病毒Gpcode.AK。該變種病毒使用了1024位元的RSA公鑰，據信在不使用分散式計算的情況下，破解該金鑰對單一電腦來說，將是徒勞無功的。

認識勒索病毒

- 加密性勒索軟體
  - 加密勒索軟體隨著2013年尾開始出現行蹤的CryptoLocker又開始了新一波的活躍期，該病毒最大的差異在於利用新時代的比特幣進行勒索。
  - 最高紀錄三天獲利2700萬美元。
  - 2017年5月，勒索軟體WannaCry (想要哭?)大規模感染了包括西班牙電信在內的許多西班牙公司、英國國民保健署、聯邦快遞和德國鐵路股份公司。據報導，至少有99個國家的其他目標在同一時間遭到WanaCryptor 2.0的攻擊。

認識勒索病毒

- 非密性勒索軟體
  - 加密勒索軟體隨著2013年尾開始出現行蹤的CryptoLocker又開始了新一波的活躍期，該病毒最大的差異在於利用新時代的比特幣進行勒索。
  - 最高紀錄三天獲利2700萬美元。
  - 2017年5月，勒索軟體WannaCry (想要哭?)大規模感染了包括西班牙電信在內的許多西班牙公司、英國國民保健署、聯邦快遞和德國鐵路股份公司。據報導，至少有99個國家的其他目標在同一時間遭到WanaCryptor 2.0的攻擊。

認識勒索病毒 – 演進史

時間	內容說明
2006年	首次出現加密勒索攻擊事件，TROJ_CRYPZIP.A**將指定類型的檔案，以密碼保護的壓縮檔打包之後，刪除原始檔案的病毒**。而這個檔案還會留下一個具有勒索文字的記事本檔案，告訴使用者可以300美元的代價，取得壓縮檔的密碼。
2011年	開始出現**鎖住螢幕要求付贖金的程式**，受害者必須撥打一個付費電話號碼，同意支付12美元的費用，才能取回系統主控權。
2012年	假冒FBI或是當地的執法機關，藉此恐嚇使用者，誤以為自己使用非法軟體，遭到警方盯上，心生恐懼而付款。
2013年	CryptoLocker勒索軟體出現，它同時採用**兩道加密方法**，第一道是以AES金鑰將檔案加密，第二道則是透過RSA演算法加密前述的金鑰，這是一種加密與解密金鑰不同的演算法，因此受害者無法直接進行反向解鎖，必須透過駭客手上的金鑰才能取回檔案，於是使用者只有兩個選擇，選擇付贖金或捨棄檔案。

認識勒索病毒 – 演進史

時間	內容說明
2014年	SynoLocker勒索軟體鎖定群暉科技(Synology)**NAS舊版DSM漏洞**進行攻擊，建議用戶更新至已修補的最新DSM版本。
2015年1月	第三代勒索軟體CryptoWall出現，造成**史上最大威脅**。據當時CTA安全聯盟估計，CryptoWall已為駭客集團帶來3.25億美元的獲利。
2015年2月	Teslacrypt勒索軟體對**某些遊戲的寶物或點數等相關檔案**，進行AES加密。
2015年11月	Linux.Encoder.1勒索軟體利用電子商務網站常用的Magento CMS漏洞，對**Linux主機資料**進行加密。
2015年11月	可離線執行、不需連到C&C伺服器的加密勒索新型態。

認識勒索病毒 – 演進史

- 從無特定對象開始轉向特定目標。
- **勒索軟體雲端化**
  - 名為Fakben的駭客團隊最近推出Cryptolocker Service勒索軟體服務
  - 只要支付50美元就能下載Cryptolocker執行檔，開始勒索事業
  - 該軟體還能設定勒索金額，以及用來收錢的比特幣帳戶
  - Fakben將索取勒索金額的10%作為服務費
  - Fakben表示，他們所關心的並非攻擊方法或目標這是客戶的責任，但他們會負責Cryptolocker的設定，而且改善Cryptolocker以躲避防毒軟體的偵測
- **勒索軟體即服務**（Ransomware as a service）
  - 暗網中已有越來越多的人宣稱提供勒索軟體作為服務，例如現在已經失效的Tox與Encryptor RaaS等

認識勒索病毒 – 演進史(雲端服務)

- **勒索軟體即服務**

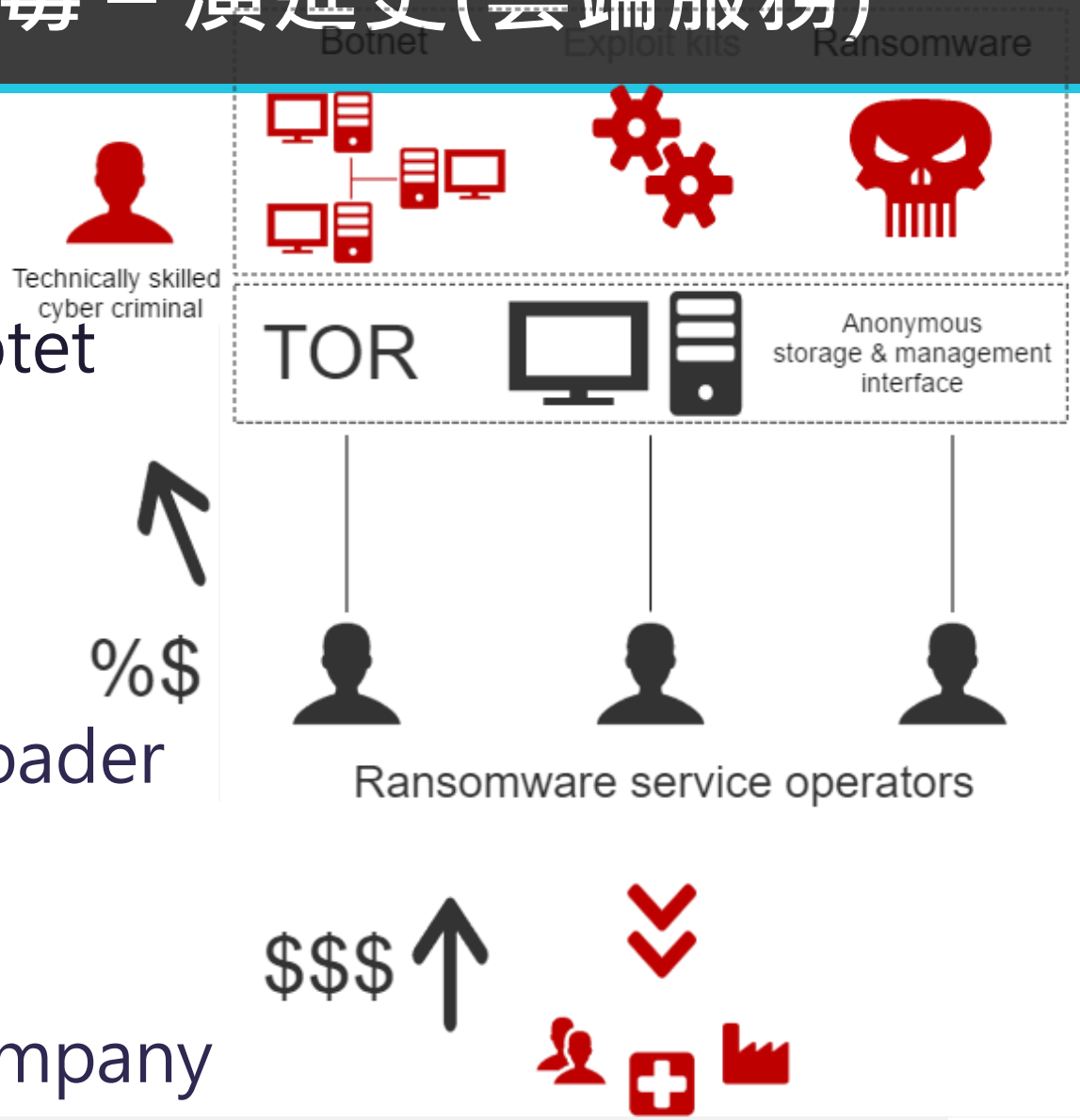
Trickbot 殭屍網路和 Emotet 惡意軟體平台

%$

Conti/Ryuk/ BazarLoader

$$$

Big Company



不付贖金，駭客無法支付更上游服務

認識勒索病毒 – 演進史(雲端服務)

- 透過惡意程式服務平臺Malware as a Service（MaaS）的傀儡網路（Botnet）上架
- 惡意程式服務平臺上架勒索軟體，支付成本相對提高
- 只有大型企業才能付得起贖金
- 企業要跟駭客殺價贖金的空間比較小
- 無良駭客——即便拿到贖金，也不打算或是無法將檔案解密

認識勒索病毒 – 攻擊對象(特定目標)

- 硬體供應鏈攻擊
- USB驅動器、乙太網連接器、微型晶片
- 引導加載程序、OTA (Over-the-Air Technology即空中下載技術）劫持
- 軟體供應鏈攻擊
- 編譯器、元件、更新器和APT

認識勒索病毒 – 攻擊對象(特定目標)

- 美國眾議院"中國工作組"於2020年9月公開之最終報告內，亦說明以下幾項供應鏈之安全必須重視:
  - 國防基礎工業
  - 稀有原料取得
  - 半導體產業生產
  - 醫療用品製造

認識勒索病毒

- 台灣常見APT族群分布
  - WaterBear、Winnti Group(APT41)、APT27 及APT10
- 攻擊延伸至相關目標供應鏈廠商
- 大量使用合法簽章或無檔案式攻擊
- **VPN**成為主要進入管道之一
- 擅長內網滲透，平均**一周內**可佔領AD
- 潛伏期長、具有連鎖反應
  - 醫院、政府單位、關鍵基礎
- 善於偽裝，使用單位合法程式
- 加殼或混淆躲避偵測與分析
- 以竊取資料為主、破壞為輔

BlackTech/WaterBear/PLEAD		
常見攻擊產業	金融、政府、醫療和科技	
常攻擊之國家	台灣、香港和日本	
常見駭客工具	Bifrost、Drigo、Kivars Plead and XBOW	
著名攻擊行動	2010	Operation Shrouded Crossbow
	2012	Operation PLEAD
	2014	Operation WaterBear
	2018	Using a valid D-LINK code-signing certificate
	2019	ASUS WebStorage

認識勒索病毒 – 針對性擄資勒贖攻擊

- ~~CPC (中油)~~
- ~~FPG (台塑)~~
- Powertech (力成)
- MIRLE(盟立)
- Unimicron(欣興電子)
- Garmin(佳明)
- Golden Bridge(金橋)
- Compal Electronics (仁寶)
- Advantech Co., Ltd (研華)
- Foxconn Technology Group(鴻海)
- Acer(宏碁)

Hackers attacked 10 listed companies in Taiwan during pandemic

Notebook giant Compal Electronics and Advantech among targets: CTWANT

2108 Like 147 Share Tweet 分享

By Matthew Strong, Taiwan News, Staff Writer

2020/12/09 14:07

認識勒索病毒

Garmin傳付贖金3億解除勒索攻擊...疫情時期駭客活動增 資安防護不足成隱憂

林 欣穎
2020年8月3日 · 2 分鐘 (閱讀時間)

仁寶疑中勒索病毒案，贖金錢包今存入約1,500 萬台幣

2020/11/22 ▪ 精選轉貼 ▪ 仁寶 、 勒索 、 加密貨幣 、 XREX 、 比特幣 、 駭客 、 洗錢 、 勒索軟體

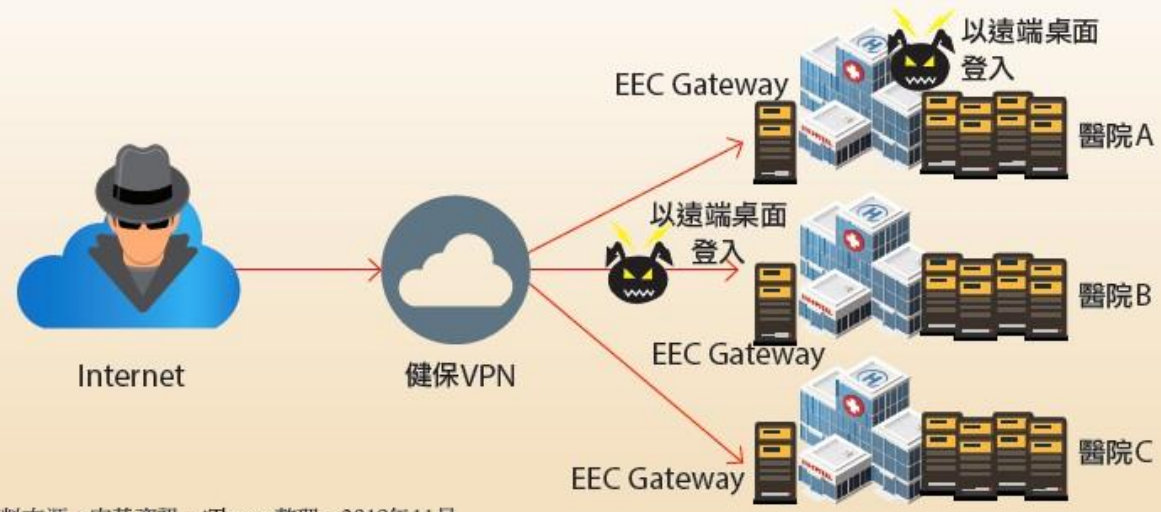
11 日 9 日，仁寶傳遭勒索軟體攻擊，但仁寶否認。11 月 19 日，贖金錢包突然存入 28.3
知由誰存入？

不付贖金就公布機密文件！勒索病毒被爆進化

讚 LINE

勒索軟體攻擊途徑借道健保VPN，同時感染臺灣多家醫院

這次多家醫療院所遭受勒索軟體攻擊，在攻擊途徑上，簡單來說，駭客先是入侵了健保VPN網路，透過衛福部的電子病例交換系統EEC，並透過遠端桌面RDP的管道感染。



資料來源：安碁資訊，iThome整理，2019年11月

認識勒索病毒

新聞

半導體封測廠力成湖口廠區遭勒索軟體攻擊，

國內大型企業接連遭駭，除了歸為關鍵基礎設施的中油，接連又傳出台塑集團出現電腦病毒攻擊，而電子業的半導體封測大廠力成也傳出

文/ 羅正漢 | 2020-05-06 發表

臺灣電子製造業遭勒索軟體再添一樁，金橋科技公告兩公司都遭勒索病毒感染

在本月下旬，國內又有上市電子製造業遭勒索軟體攻擊，我們近日在臺灣證券交易所公開資訊觀測站，發現連接線組製造商金橋科技發布

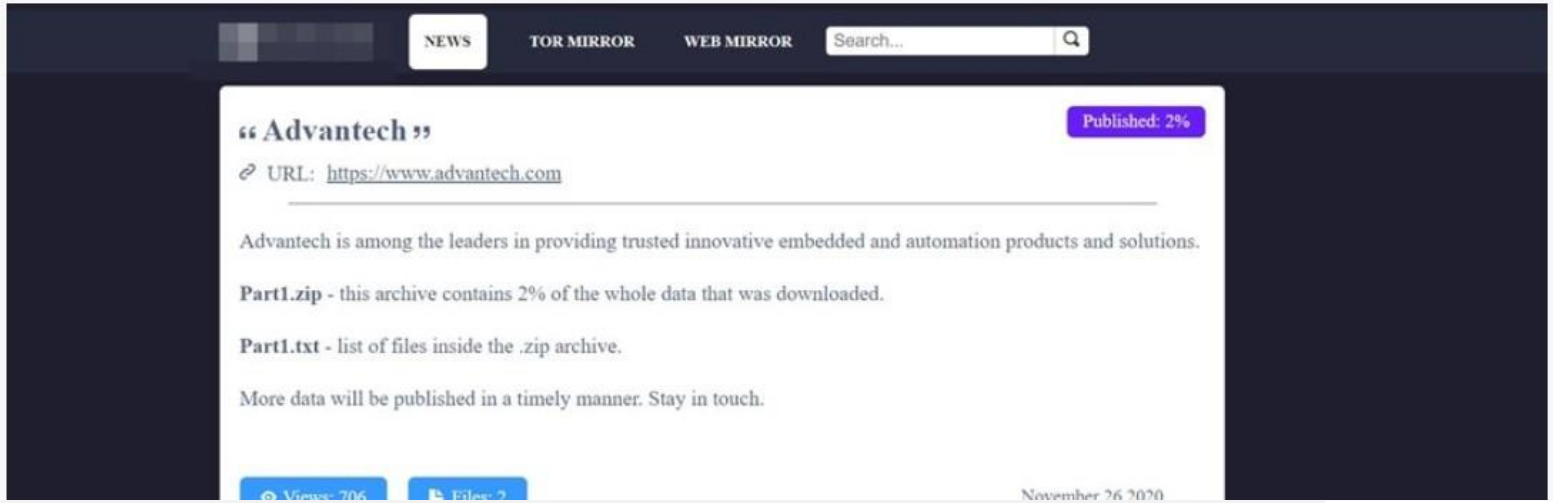
文/ 羅正漢 | 2020-08-28 發表

Conti勒索軟體駭客曝光一批3GB內部資料，宣稱偷自研華

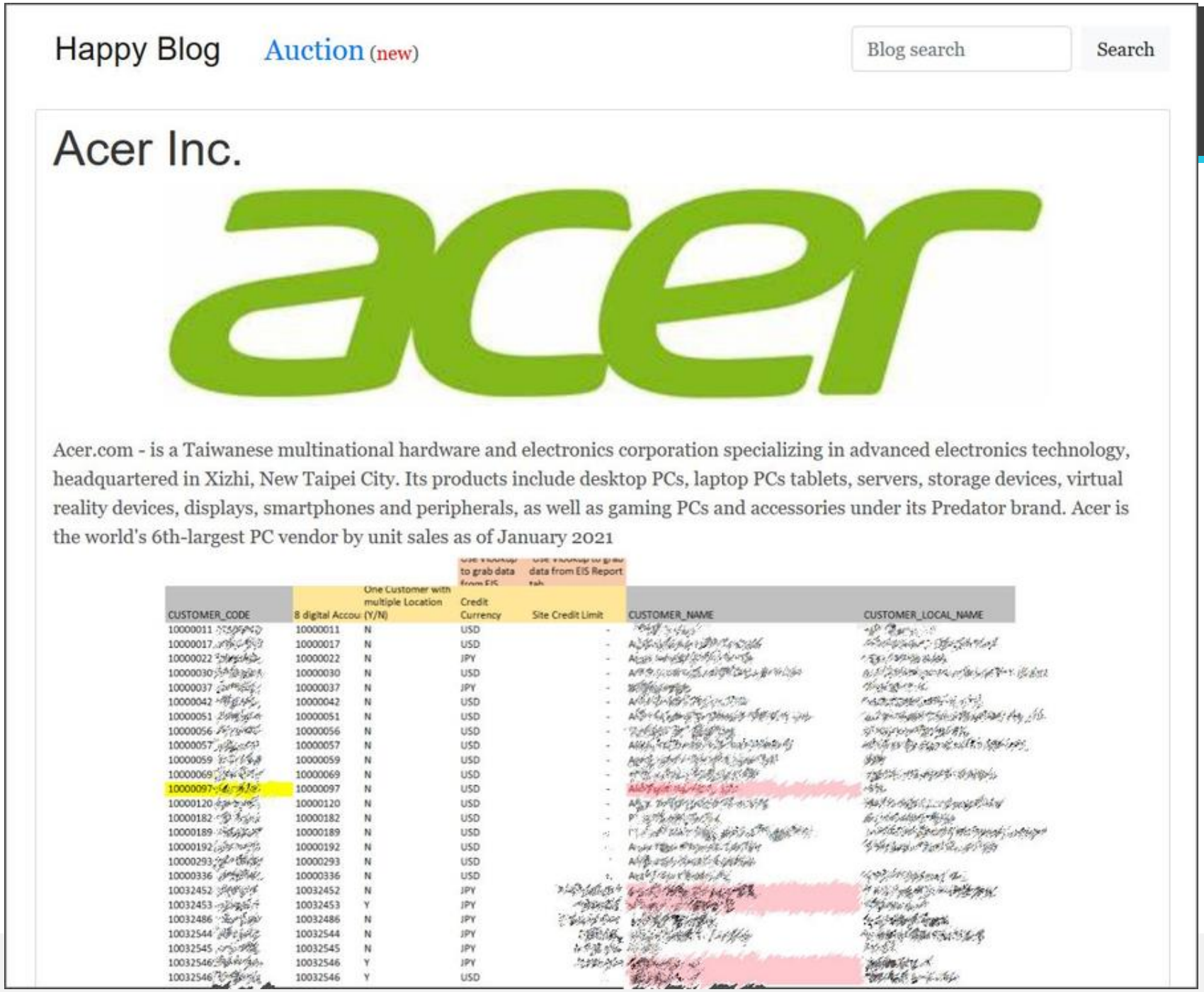
駭客勒索沒有成功，轉而於11月26日公布了宣稱自研華竊取的3GB檔案和檔案目錄清單文字檔，這些資料占他們所偷走資料的2%，但受害企業沒有證實

文/ 陳曉莉 | 2020-11-30 發表

讚 6.3 萬 按讚加入iThome粉絲團 讚 185 分享



認識勒索病毒

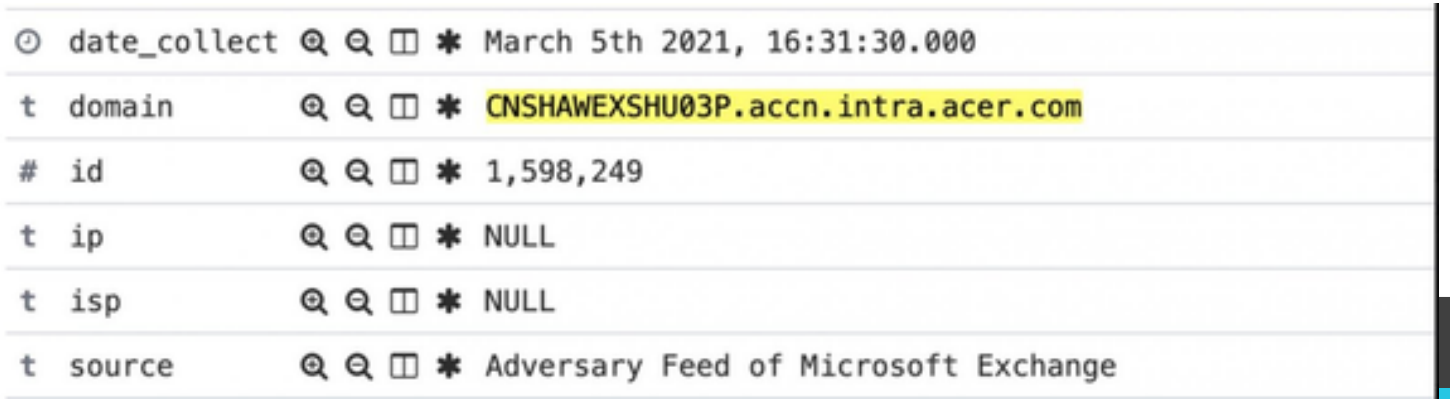


2021年3月20日

勒索軟體駭客組織REvil宣稱，他們攻擊電腦大廠宏碁，並公布疑似內有竊得資料的螢幕截圖，駭客向宏碁勒索5千萬美元贖金，約相當於新臺幣14億元。

認識勒索病毒

- 外洩內容，包含了財務報表、帳戶餘額，以及與銀行之間往來的相關文件
- 索討約5千萬美元，是目前為止REvil開出最高的贖金金額
- 駭客要脅若是沒有在期限內付錢，贖金就會翻倍到約1億美元
- 鎖定一臺位於宏碁網域的Exchange伺服器，而且疑似濫用ProxyLogon 漏洞
- 是首度濫用相關漏洞的大型勒索軟體攻擊



認識勒索病毒－四大威脅趨勢

入侵機構內部重要資源

- 造成網域控制器(DC)或目錄服務(AD)中斷，迫使企業支付贖金。

不僅加密亦竊取檔案

- 將檔案傳送至駭客組織，使企業承受資料外洩壓力。

認識勒索病毒 – 四大威脅趨勢

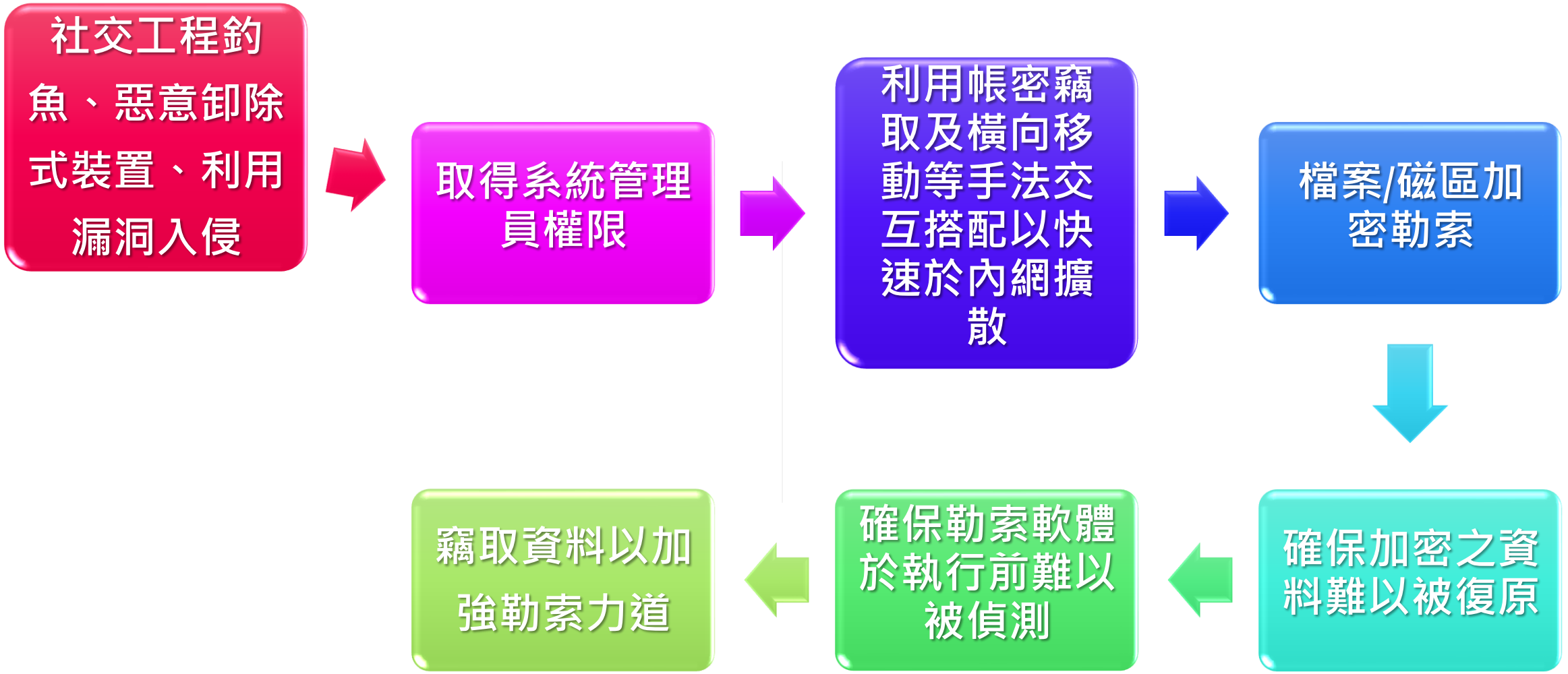
駭客組織彼此結盟，將攻擊企業化

- 駭客組織與提供「存取服務」（出租或銷售各種機構的網路存取權限）之不肖業者合作

威脅持續攀升

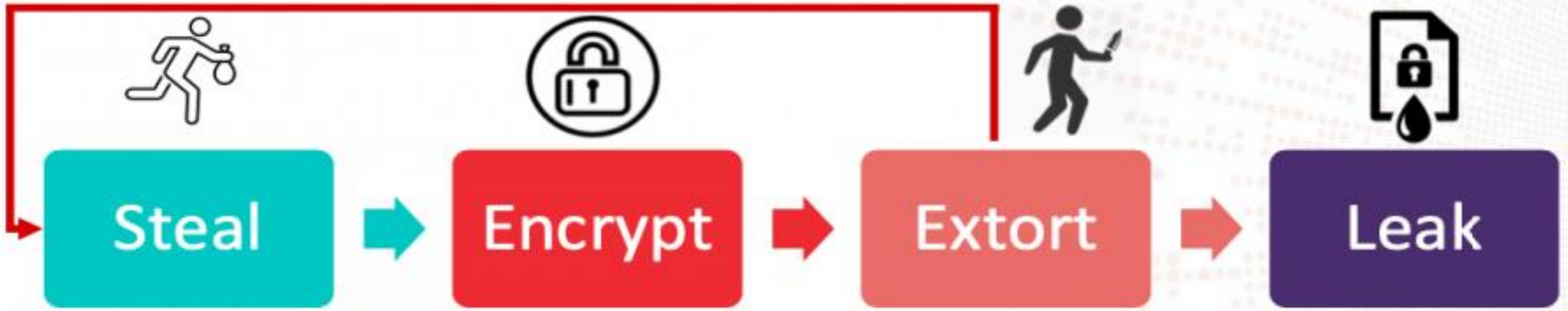
- 近期勒索軟體威脅數量持續成長

認識勒索病毒－7步驟攻擊流程



認識勒索病毒 – SEEL

升級為勒索四部曲S.E.E.L



使用APT手法入侵
攻擊大部分人為操作
鎖定單位AD主機
鎖定重要資料
HR、SAP、MES、Accounts
傳輸到雲端硬碟

AD部屬加密程式
AD設定定時炸彈
實施檔案加密階段

暗網攻擊新聞發布
寄給單位IT人員勒索訊息
持續竊取資料

逐步洩漏資料
公布洩漏進度比

認識勒索病毒 – SEEL

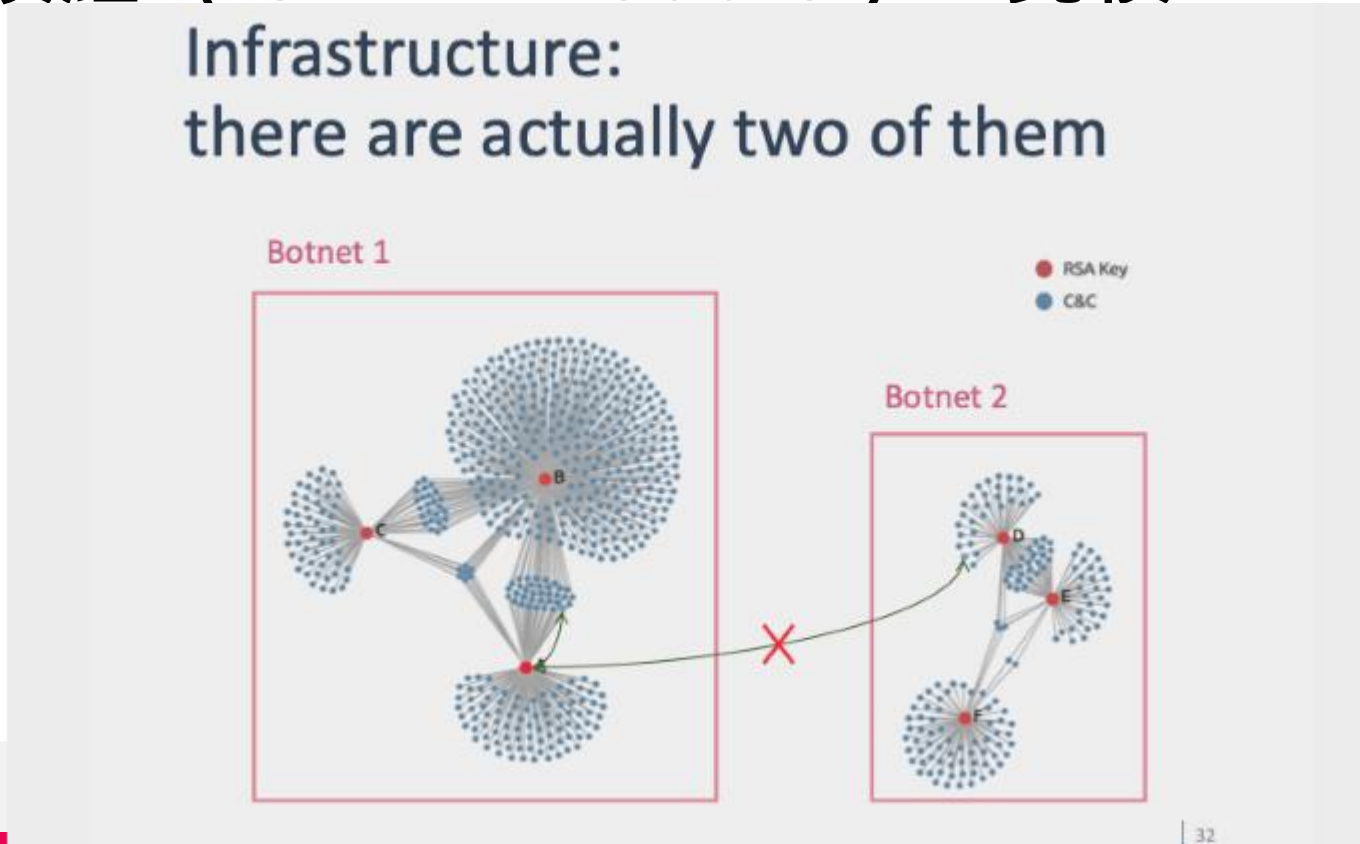
- 勒索軟體為了提高勒索的成功率，也開始數位轉型
- 開始鎖定大型企業作為狩獵（Big game hunter）標的
- 確保被勒索的企業，有能力且有意願支付勒索贖金
- 比特幣解決以往駭客集團最傷腦筋的金流問題
- 「雙重勒贖」的作法
  駭客透過加密檔案以及外洩機敏資料的雙重手法，確保企業一定肯支付贖金的作法，就是雙重勒贖

認識勒索病毒 - Emotet

- 最早在2014年就是一個金融木馬的駭客組織
- 後來慢慢轉型，成為提供網路犯罪基礎架構
- 提供相關惡意程式與工具的幕後黑手
- Emotet 中繼站設計成多層次網路架構：
  - 第一層為受 Emotet 感染的受駭主機
  - 第二層通常架設於被入侵的網站伺服器上
  - 第三層（目前主流共識的研判）為黑客實際註冊的伺服器
  - 讓執法單位拔除整個傀儡網路的難度更高之外，也使外界更難窺得完整的網路架構

認識勒索病毒 - Emotet

- 第一層的中繼站為受感染的電腦，這些電腦時常隱藏在區域網路（NAT）內部
- 從中繼站派送通用隨插即用模組（UPNP Module），此模組會向區域網路的路由器來註冊通訊埠轉發（Port Forwarding）讓外網受感染的機器可與位於內網的傀儡電腦進行溝通。
- 透過自動化方式完成相關惡意程式的派送和部署



認識勒索病毒 - Emotet

- 事實上，若單就Emotet而言，也是最惡名昭彰的垃圾郵件傀儡網路。
- Emotet有三種主要的傳播方式：
  - 透過帳號密碼竊取模組（Credential Stealer Module），將受害者電腦上的帳號、密碼傳送回中繼站
  - 使用郵件竊取模組（Email Stealer），將受害者電腦上的信件傳送回中繼站，再從信件中，獲得攻擊目標的資訊
  - 垃圾郵件發送模組（Spamming Module），從受害者電腦上登入被竊取的郵件信箱帳密，並自動寄出垃圾郵件
- 採用社交工程技巧，並可能使用合法的電子郵件地址發送

認識勒索病毒 - Emotet

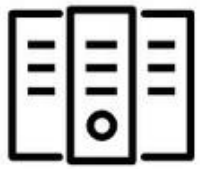
- COVID-19在俄羅斯肆虐的那段期間，很多惡意活動都處於停止或類似休眠的狀態，但後來隨著封城措施逐步解封，又陸續活躍起來，這些網路犯罪集團的本業，極可能有實體辦公室
- 愛用時下當紅話題來誘騙受害者手段，使用大量與COVID-19相關郵件主題，來攻擊受害者，甚至包含各種醫療機構在內。
- 八國聯手抄底Emotet

認識勒索病毒 – Emotet阻擋清單

- 一旦察覺內網對外連線到下列IP位址，應該要盡速請資安事件調查專家介入：
  - 80.158.3.161:443
  - 80.158.51.209:8080
  - 80.158.35.51:80
  - 80.158.63.78:443
  - 80.158.53.167:80
  - 80.158.62.194:443
  - 80.158.59.174:8080
  - 80.158.43.136:80

認識勒索病毒 – 中毒之現象

Your network has been infected!



Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

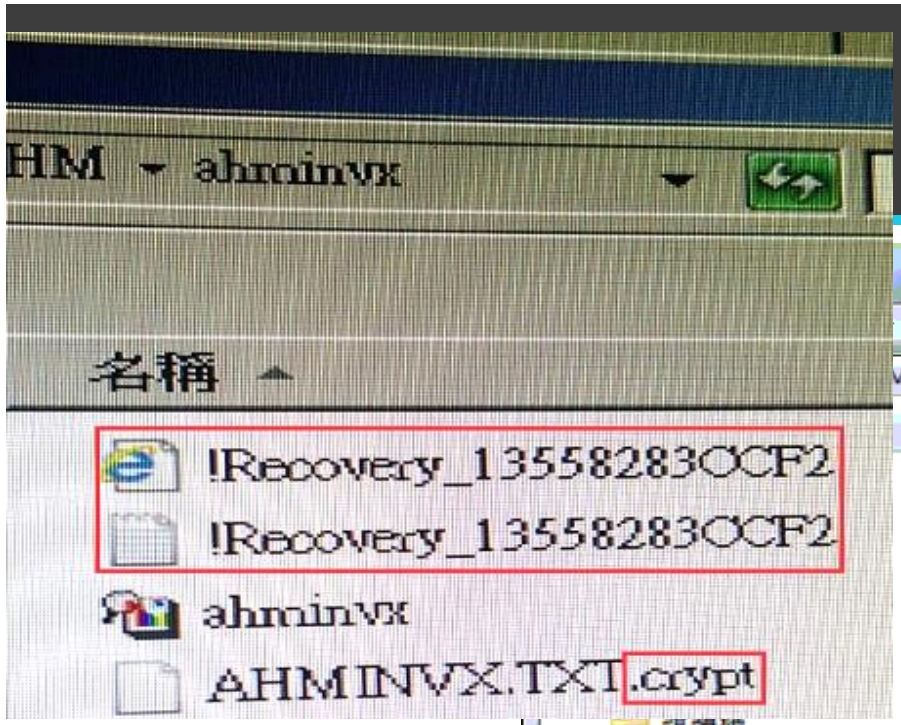
You have 8 days, 19:07:29

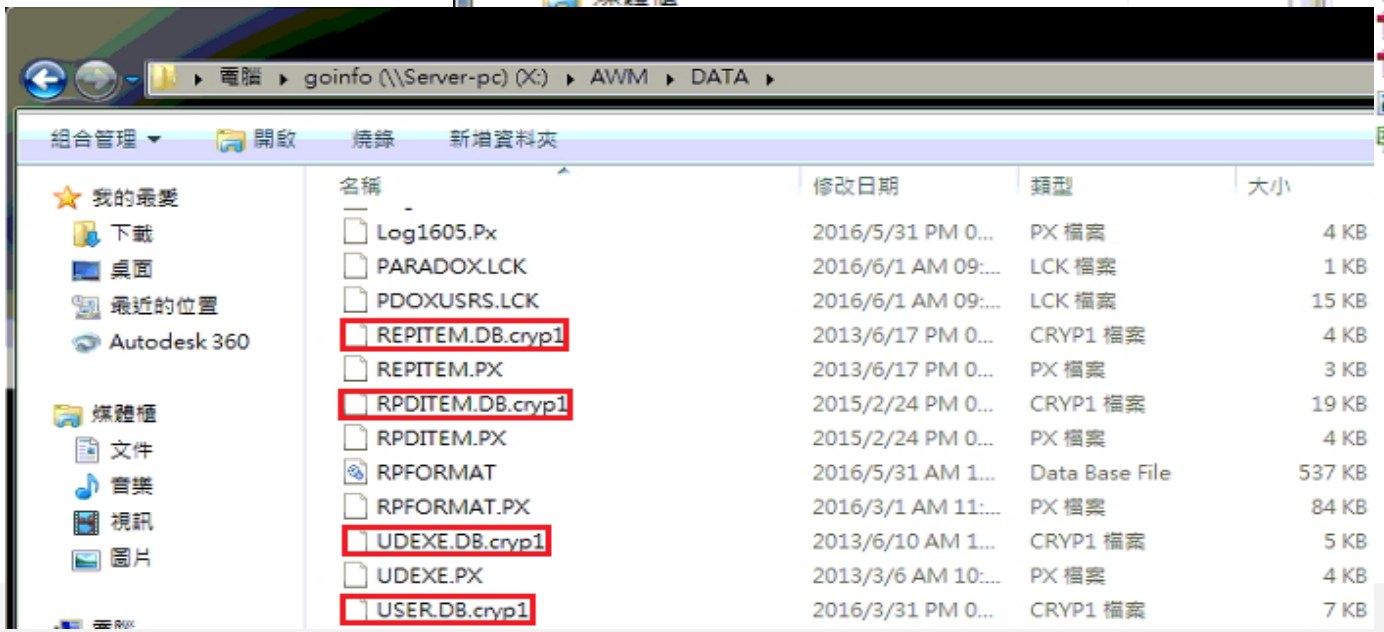
* If you do not pay on time, the price will be doubled
* Time ends on **Mar 28, 16:30:11**

Current price: 214151 XMR ≈ 50,000,000 USD

After time ends: 428302 XMR ≈ 100,000,000 USD

認識勒索病毒 – 中毒之現象





認識勒索病毒－影響

- 破壞資訊系統
- 竊取機密敏感資料
- 中斷網路服務
- 以加密方式綁架電腦檔案與資料夾

勒索軟體安全防護

Security protection against ransomware

認識勒索病毒 – 面對Emotet的解決之道

- 荷蘭警方有提供電子郵件查驗的服務，可以確認個人使用的電子郵件是否是Emotet用來濫發垃圾郵件的傀儡電腦
  https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html

認識勒索病毒 – 面對Emotet的解決之道

- 防範社交工程，使用者要避免打開未知或可疑的電子郵件
- 防毒軟體的掃描是不可或缺的基本工具
- 保持使用者電腦系統更新
- 加強密碼複雜度，並定期更改密碼
- 強化VPN管理
- 遠多桌面連線跳板機與第二重認證

提供的防護功能

保護檔案免受勒索軟體等的威脅，並了解

受控資料夾存取權

保護檔案、資料夾及記憶體區域，避免不
變更。

4

開啟

封鎖歷程記錄

受保護資料夾

允許應用程式通過受控資料夾存取權

有任何疑問嗎?

取得協助

協助改善 Windows 安全性

提供意見反應給我們

Windows 安全性

病毒與威脅防護

保護您的裝置免受威脅。

目前的威脅

沒有目前的威脅。

上次掃描: 2021/2/19 下午 12:38 (快速掃描)

發現 1 個威脅。

掃描持續 2 分鐘 30 秒

51107 個檔案已掃描。

快速掃描

掃描選項

允許的威脅

保護歷程記錄

病毒與威脅防護設定

不需採取動作。

3

勒索軟體防護

不需採取動作。

管理勒索軟體防護

Windows 安全性

安全性概覽

請查看您裝置的安全性和健康情況，並採取任何所需的動作。

2

病毒與威脅防護
不需採取動作。

帳戶防護
不需採取動作。

防火牆與網路保護
不需採取動作。

應用程式與瀏覽器控制
不需採取動作。

裝置安全性
檢視狀態和管理硬體安全性功能

裝置效能與運作狀況
不需採取動作。

1

Windows 安全性

勒索軟體安全防護 – 平常之防護原則

- 重視資料備份(備份後切斷連線)
  - 主機備份(Server RAID陣列或一般PC備份等)
  - 異地備份(資料同步至NAS或雲端硬碟等)
  - USB隨身硬碟備份(將資料額外複製到快閃隨身碟)
- 作業系統或應用程式定期修補、更新
  - 勿使用來路不明的軟體，程式跳出更新通知時請勿立即執行更新
  - 駭客常利用Windows、Java、IE及Flash漏洞來進行攻擊，應時常更新
  - 更新設定：通知安裝，自我選擇安裝

勒索軟體安全防護 – 平常之防護原則

- 強化資安意識，可疑文件與連結不能點
  - Facebook、Line等社群軟體的連結切勿因好奇而隨意亂點
  - 可疑郵件及其附件檔案要審慎確認後再決定是否開啟
- 安裝相關防毒軟體並注意保持更新
  - 建議安裝可信賴的防毒軟體(Kaspersky、NOD32、Norton或PC-Cillin等)
  - 不建議安裝對岸的防毒軟體，因其容易藏有木馬或廣告綁架程式
- 重新檢視公司內部的使用存取權限
  - 公司資訊人員可利用網域或權限功能來防止使用者任意安裝程式或使用私人隨身碟

勒索軟體安全防護 – 10點防護基礎架構

定期備份重要資料	•重要資料應進行異地備份及離線備份，建立災害復原程序
落實資訊資產盤點	•盤點整體資訊資產，確實掌握網際網路可存取之設備
落實網段配置安全管理	•依風險將主機置於不同網段，避免跨網段主機任意連線
加強特權帳號管理	•如透過雙因子認證、檢視帳號使用與管制、禁止共用等

勒索軟體安全防護 – 10點防護基礎架構

管控遠端存取服務	• 限制存取服務之來源、時間、避免連接到本地資源
強化對外服務資安防護	• 將對外服務納入資安設備防護範圍，並加強監控
落實情資驅動防護	• 及時分析資安情資，並採取對應之預防及應變措施
強化資安監控作業	• 搭配資安情資分析系統日誌，若有異常則啟動應變機制

勒索軟體安全防護 – 10點防護基礎架構

提升CSIRT團隊職能	• 建立勒索軟體應變及災害復原程序，並定期演練
強化員工資安認知訓練	• 定期執行社交工程演練及教育訓練，確保員工能及時應變

勒索軟體安全防護 – 遭受攻擊之處置原則

遭受勒索軟體攻擊時的處置原則：

- 立即清查內部遭受攻擊的電腦
- 中斷網路連線、關閉電腦
- 評估受攻擊電腦的感染程度
- 將未被加密的重要資料盡速備份出來
- 重灌系統或支付贖金
- 加強宣導如何防範勒索軟體的攻擊及平時備份的重要性

勒索軟體安全防護 – 遭受攻擊之處置原則

- 如發生資訊安全事故，應依據「政府機關（構）資安事件數位證據保全標準作程序」進行數位證據之蒐集與保存，如電腦稽核軌跡及相關的證據，應以適當的方法保護，以利於下列作業：
  - 作為機關內部分析問題之依據。
  - 作為研析是否違反契約或是違反單位資訊安全規定的證據。
  - 作為與軟體及硬體供應商，協商補償之依據。

勒索軟體安全防護 – 遭受攻擊之處置原則

- 企業為了即時恢復系統運作，電腦重灌成為最常見的手法
- 駭客入侵的軌跡和相關的登錄檔（Log）
- ISO/IEC 27001:2013 附錄A.16資訊安全事故管理相關要求

A.16.1.6	從資訊安全事故中學習	控制措施 藉分析與解決資訊安全事故獲得的知識應用，以降低未來事故的可能性或衝擊
A.16.1.7	證據的收集	控制措施 組織應對可作為證據之資訊，明定適用的識別、收集、獲取及保存程序

總結

Conclusion

結　語

強化組織資安防護能力，達成安全、便利、營運不中斷

- 全球各機構遭受勒索軟體攻擊頻率持續增加
- 全球各機構觀察到勒索軟體威脅持續上升
- 應強化及落實防護機制，並加強監控相關威脅
- 應落實資料備份，包含異地備份及離線備份

現代防疫(駭)學

- 零信任 Zero-trust → 持續檢查
- 主動防護 Proactive → 向他人學習 (情資分享)
- 預警防護 Predictive → 向行為者學習
- 資安韌性Resilience → 及時回應
- 資安勢態Posture→ 持續遵守相關要求

結　　語

- 雖然勒索軟體的威脅無法被完全革除，使用IT業界所稱的多層次預防策略（defense-in-layers security strategy）卻稱得上是不錯的預防手段。多層次預防策略提倡同時部署多種獨立、領域互相重疊的安全措施以建立穩固的安全措施。各安全層被設計和其他安全層互補，使得威脅不易穿透重重防護。例如一個安全策略可能包含下列五層：
- 全面性的、完備的安全政策
- 網路和郵件的內容過濾代理伺服器
- 限制級別存取
- 以密碼上鎖特定功能
- 不間斷的員工警覺性訓練

課程結束．感謝參與

方煥文

0935-701552

arvin.fang@msa.hinet.net

博創資訊科技股份有限公司