2017
IoT時代，使用者的資安2.0

Agenda

- 引言
- 資安威脅趨勢
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

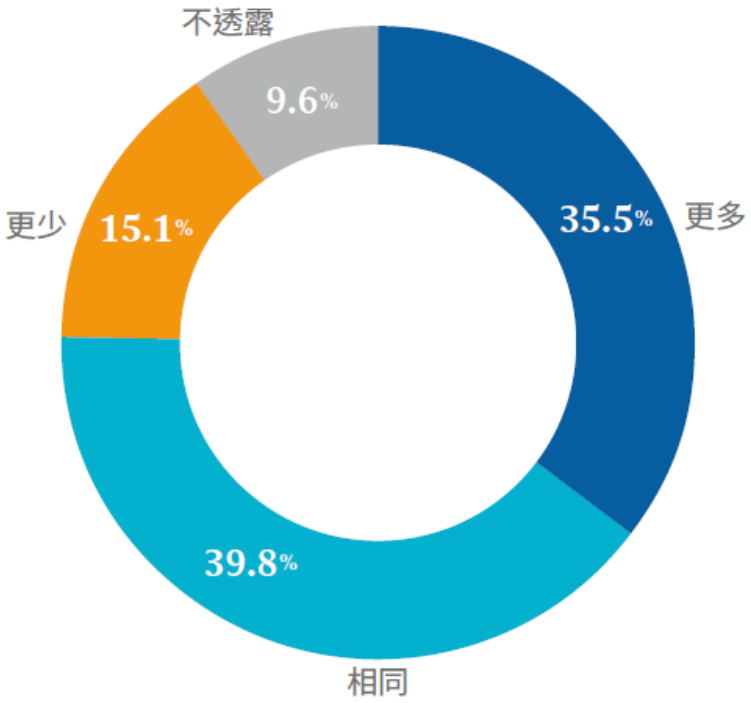
美國聯邦調查局局長:企業只有兩種....

已經遭駭客入侵

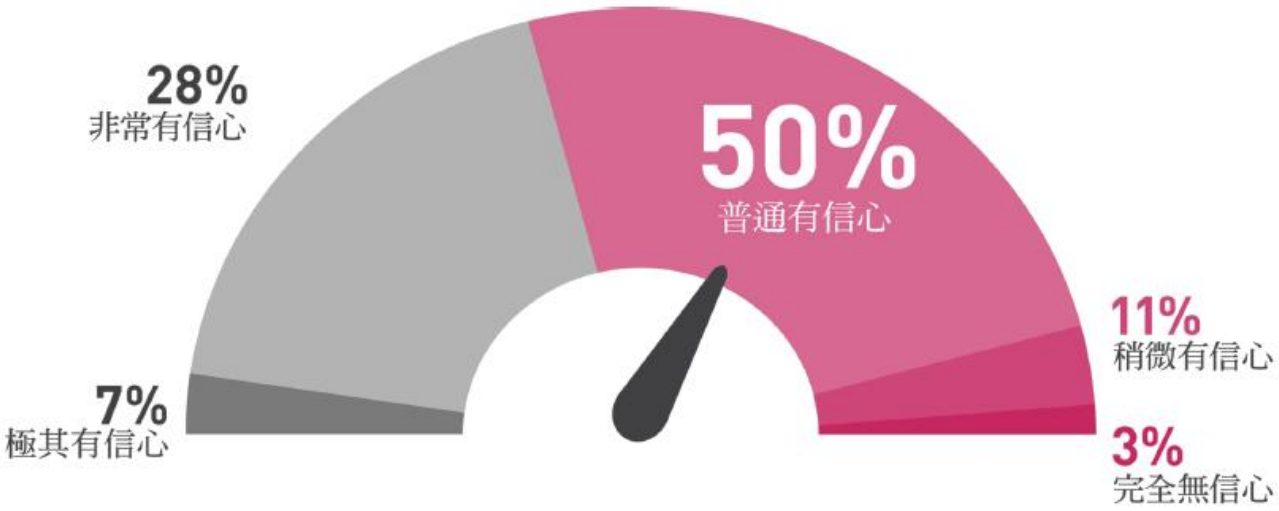
遭駭客入侵卻沒發現

企業資訊安全調查

企業IT資安投資金額...

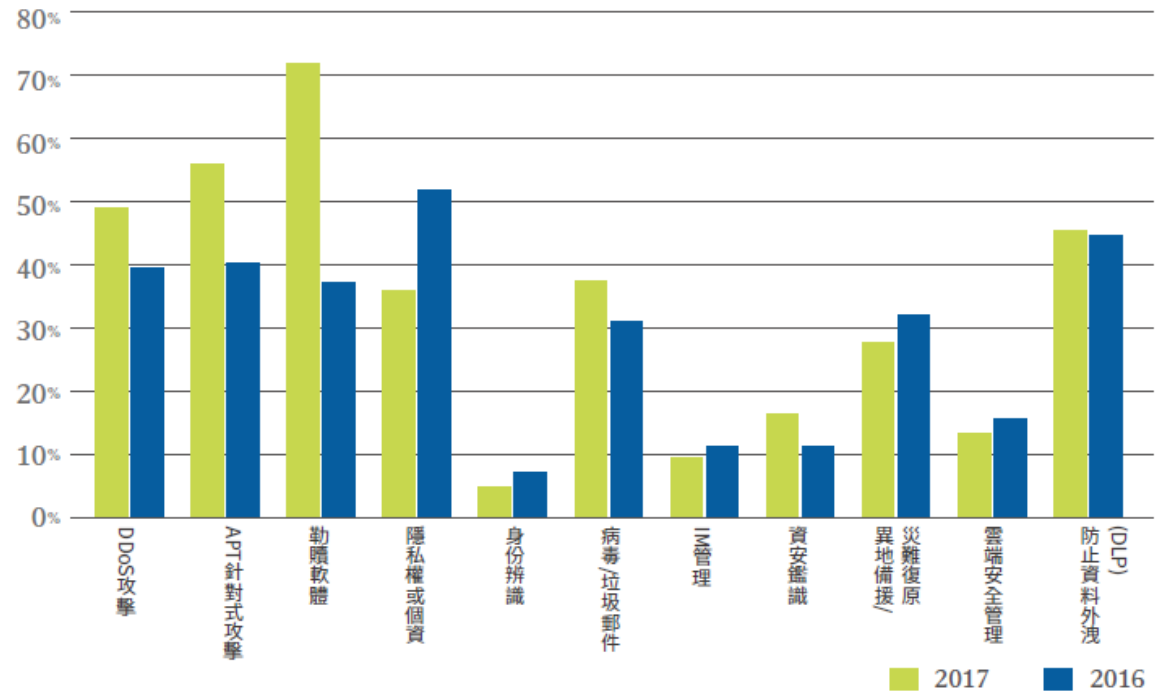


企業資安防護信心度?



2017資安防護需求調查

調查結果呈現了威脅項目的消長。勒贖軟體大爆發，從個人至企業都是冷汗直流。而隱私權問題就像個重要但不迫切的項目。



資安未來攻擊趨勢

Agenda

- 引言
- 資安威脅趨勢
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

Agenda

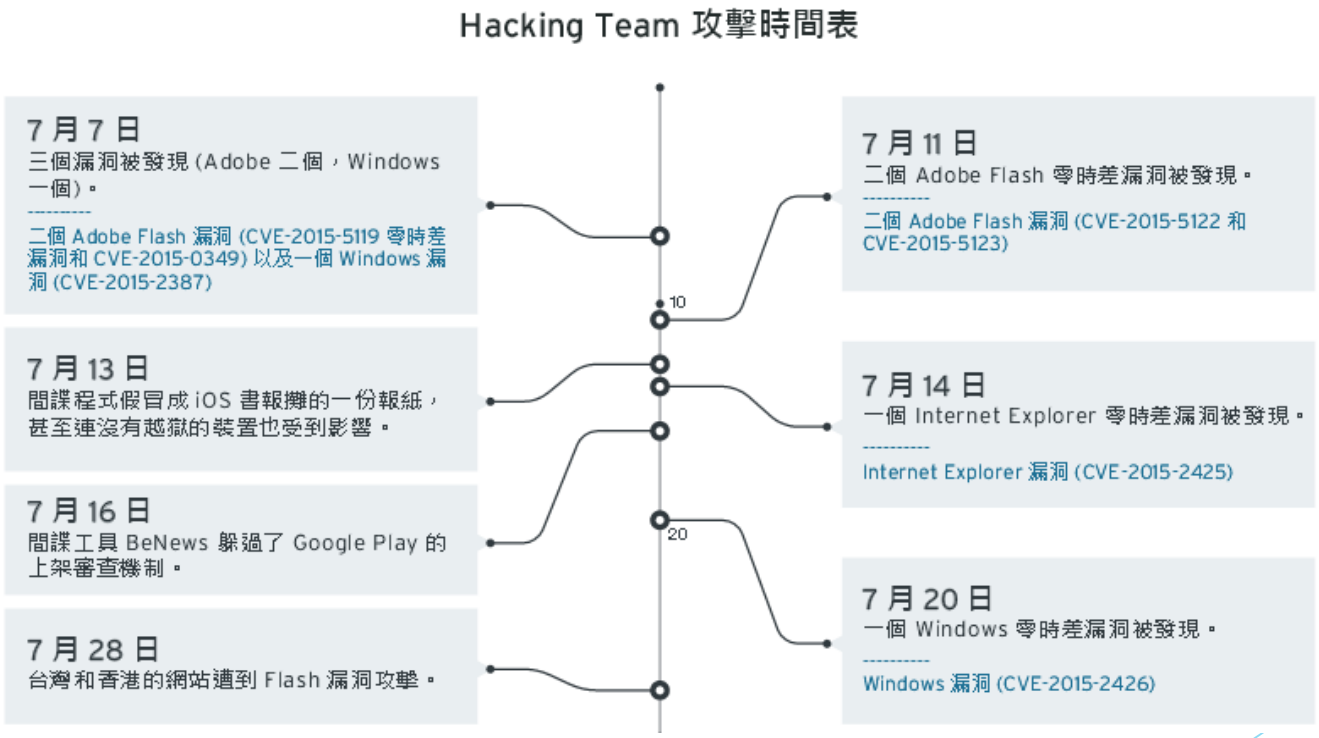
- 引言
- 資安威脅趨勢
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

今[illegible]開

事件摘要　2015 年7月，專門協助各國政府執行監控任務並開發間諜軟體的義大利公司Hacking Team遭駭，外洩了400GB內部機密資料，內有該公司長期蒐集如微軟、Adobe或是其他系統的零時差漏洞，也有與各國政府往來電子郵件，也包括了美 國、歐洲或聯合國所列的黑名單國家或極權國家，其中也有來自臺灣詢價往來郵件。

主要影響　外洩資料包括了多項零時差漏洞，成了其他駭客發動攻擊的強大數位軍火庫，也促使微軟、Adobe等公司緊急修補被公開的零時差漏洞。多國政府向Hacking Team購買監控工具的交易因此曝光，也造成了各國內政局不安。

HackingTeam資料外洩:
有如一座滿是系統漏洞的寶藏




TANet
COMPUTER EMERGENCY RESPONSE TEAM
台灣學術網路危機處理中心
TAIWAN >>>
TANet CERT台灣學術網路危機處理中心
回首頁
即時訊息
安全通報
資安通報
網路資源
資安文件
關於我們
最新安全通報
2017-06-09
Cisco 存在多個安全性弱點....
2017-06-09
VMware vSphere ....
緊急公告 Emergency
因應校園網路勒贖處置說明(點我下載) 2017-02-22
教育部自2月16日起透過台灣學術網路危機處理中心(TACERT)，發送資安事件警告通報各校，
並呈報行政院，同時彙整收到駭客恐嚇信學校清單。建議各級學校採取適當防護措施，
若有問題及疑慮，請立級透過「教育機構資安通報應變平台」進行通報，教育部將即時掌握受害情況。
勒索軟體 WanaCrypt0r 2.0攻擊事件建議處置作為(點我下載)2017-05-13
對 勒索軟體WanaCrypt0r 2.0建議處理方式，請參考下列文件進行處理：文件下載
http://tacert.tanet.edu.tw/prog/index.php
最新消息 NEWS
2017-06-16 [國際]WannaCry肆虐全球時，Rapid7：全球網路有超過500萬個開放的SMB節點
2017-06-15 [技術]卡巴斯基找到勒索軟體Jaff的漏洞，釋出解密工具
2017-06-15 [技術]Dvmap：第一款利用程式碼注入的Android惡意軟體
資安通報
click here
連絡我們 MAIL
殭屍網路
惡意程式
隱私權聲明
TACERT統計報表
網站連結
教育部
校園資訊安全服務網
教育部
資訊及科技教育司
www.edu.tw

https://www.twcert.org.tw/

TWCERT/CC

Taiwan Computer Emergency Response Team / Coordination Center

首頁 | 資安新聞 | 資安新知 | 資安通報 | 網路資源 | CERT組織 | 關於我們

最新資安新知

- Drupal發佈安全更新，部分漏洞會導致執行任意程式碼
- Windows NTFS漏洞，可能導致阻斷服務
- VMware發佈安全更新，該漏洞會導致權限提升
- Joomla!發佈安全更新，該漏洞會導致SQL注入
- 微軟惡意程式防護引擎(Microsoft Malware Protection Engine)存在...

台灣電腦網路危機處理暨協調中心(TWCERT/CC)自八十七年九月正式成立以來，為了防止電腦網路安全危機的發生，即積極協助台灣地區電腦網路安全相關事件、協助系統管理者診斷電腦網路安全漏洞、建置網站以提供電腦網路安全資源，及舉辦網路安全之宣導活動等。

TWCERT/CC秉持作為國內首度關切電腦網路安全單位的宗旨，在加速電腦網路安全相關資訊流通、提升網站安全等級、提供相關教育訓練課程等方面提昇服務效率，以期推動電腦網路安全相關之工作事項。

TWCERT/CC希望能夠成為全台灣處理網路安全方面事件的對外窗口，擔任起與世界各國 CERT 組織溝通的任務，以提供國人更完善之服務與安全訊息，並與其他國家共同為網路安全盡一份心力。

最新資安新聞

- [國際]使用影音撥放器撥放字幕要小心，駭客透過撥放器漏洞可執...
- [國內]雄獅36萬筆個資外洩 駭客主要來自中國
- [國際]Microsoft Windows作業系統及Google Chrome瀏覽器存在處...
- [國際]HKCERT警告：特別防範一種透過惡意 PDF 附件傳播、名...
- [國內]金管會資安中心將於下月成立

台灣電腦網路危機處理暨協調中心

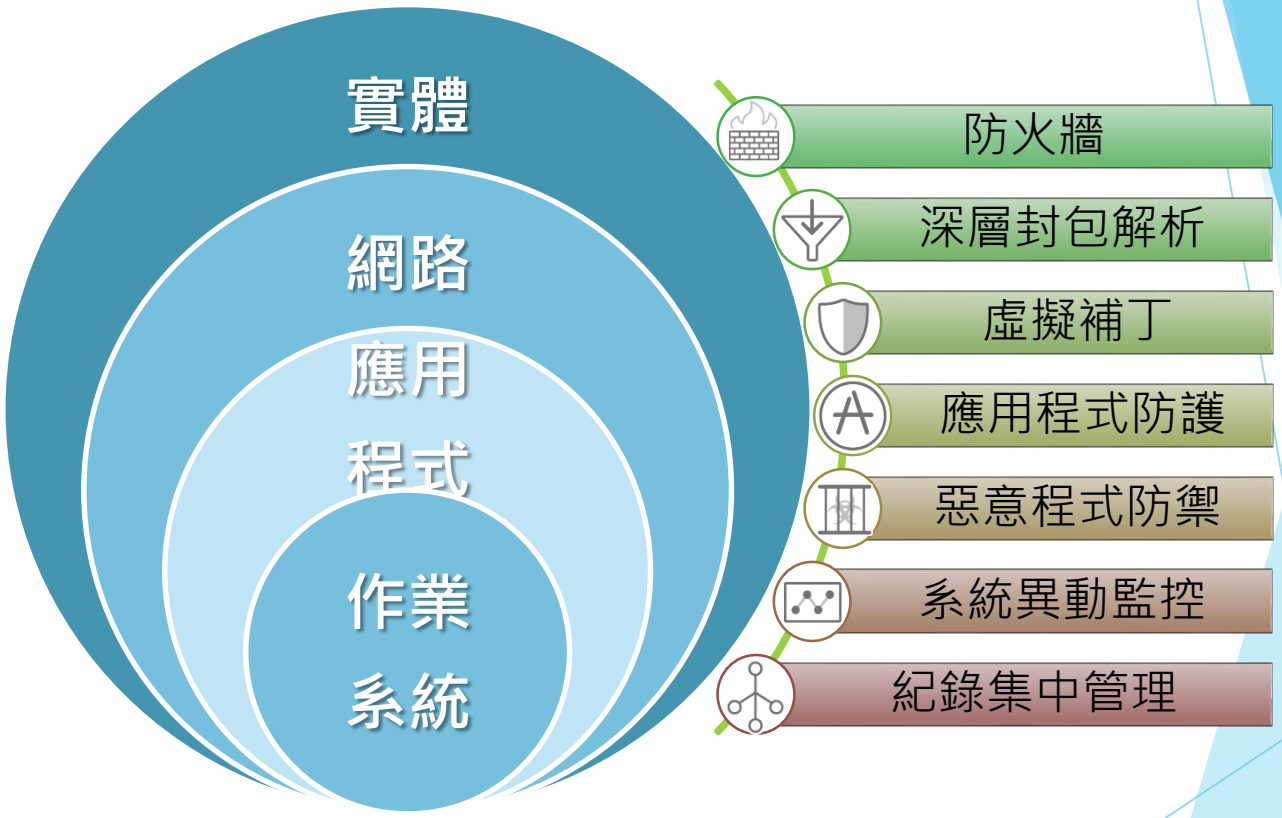
桃園辦公室
免付費服務電話 0800-885-066
資安事件通報 03-4115387
傳真 03-4713363

臺北辦公室
資安事件通報 02-23776418
Email:twcert@cert.org.tw

Copyright © TWCERT/CC 台灣電腦網路危機處理暨協調中心 1998-2016

- 網路環境正日益惡化，而且**攻擊不再只是單一事件**。
- 企業必須調整自己的資安事件**應變計畫來應付第二階段的攻擊**，包括二次感染或利用偷來的資訊進行恐嚇勒索。
- 抑制駭客的入侵行動將成為事件應變的目標，能**降低駭客潛伏的時間**，必須**破壞主機上建立據點**的能力，進而防止駭客感染。

打造一個適應性安全架構



Agenda

引言

資安威脅趨勢

- 資料外洩助長攻擊和勒索
- 潛藏的禍害
- 未來的隱憂 - IOT Security

網路勒索之年

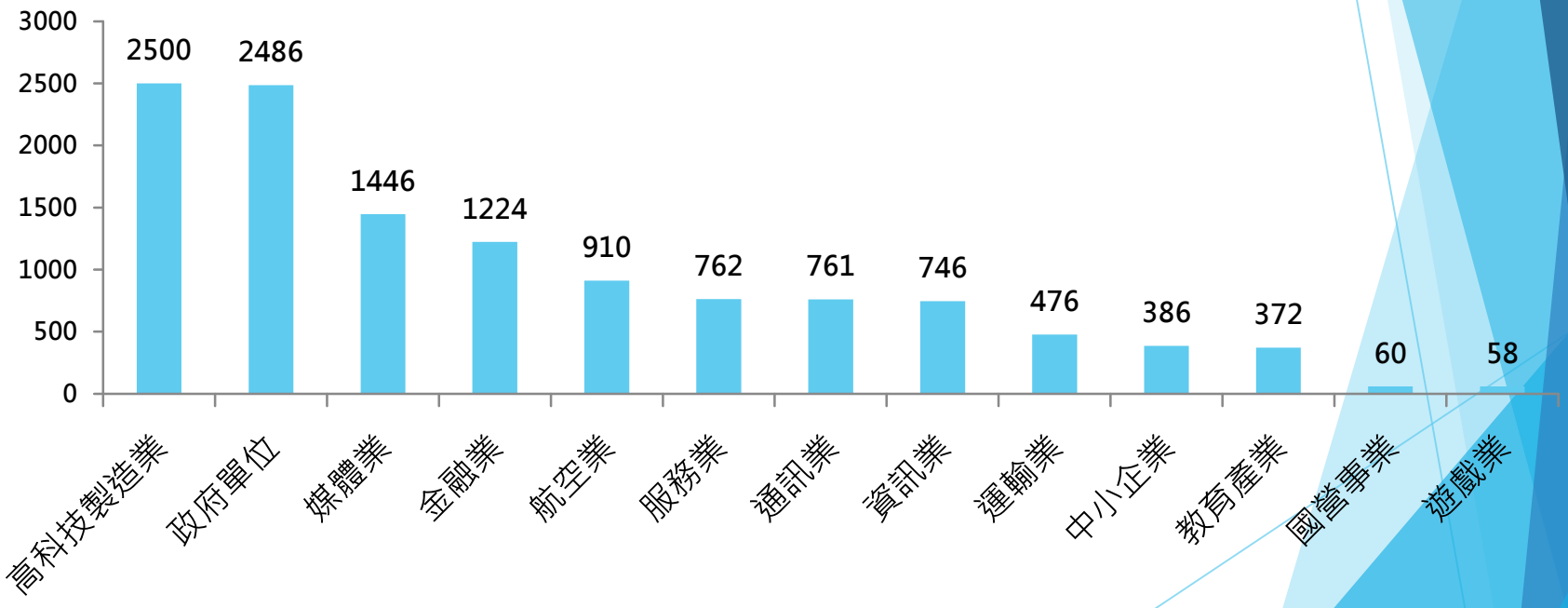
案例分享

如何因應與面對

Q&A

台灣各產業面臨嚴峻的駭客入侵資安威脅

- 趨勢科技共調查413個駭客入侵案件，檢查2267台電腦
- 前三名受駭嚴重產業：高科技製造業、政府機關、媒體業，其中高科技製造業可能被駭客入侵後2500天才發現異常狀況，進行處理

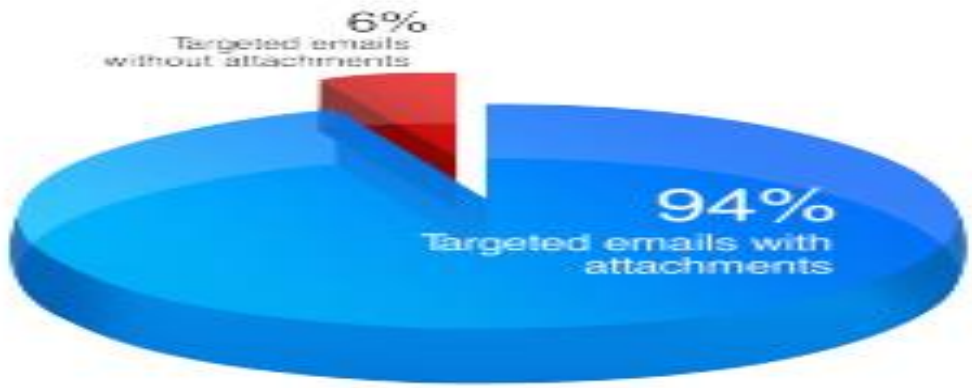


為什麼防不勝防?

人性的弱點

社交工程攻擊

APT入侵最有效也最簡單的方式-社交工程電子郵件

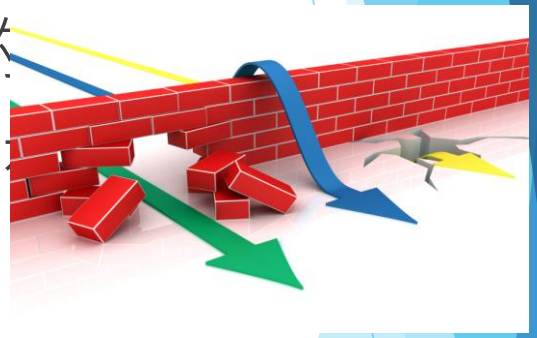


為什麼防不勝防?

刻意躲避偵測的
客製化攻擊

傳統防禦機制失靈

- 防毒軟體無法辨識 APT
  - APT的惡意程式幾乎都是客製化的
    - 利用系統或文件軟體漏洞，甚至
      時差弱點
- 防火牆完全無效
  - 利用正常的通信埠及通信協定
- 入侵偵測無效
  - 網路流量正常，小量批次傳送資料

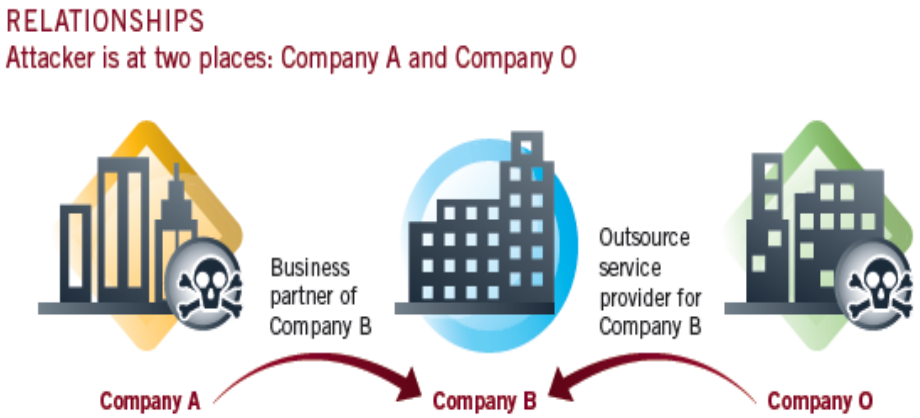


為什麼防不勝防?

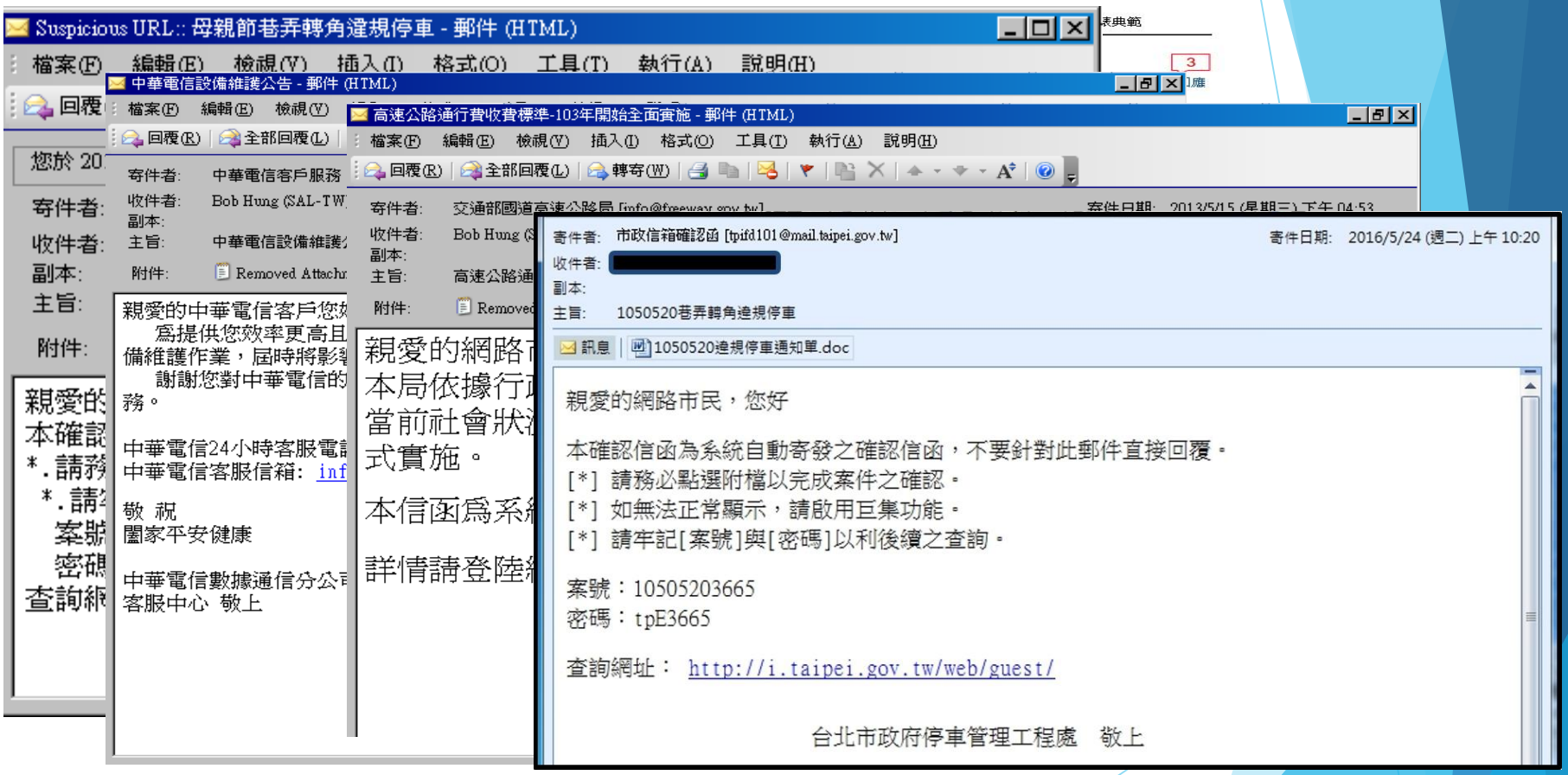
低調迂迴、契而

由於APT低調隱密
將近50%以上的受害組織毫無查覺

APT攻擊具有「誅九族」的特性



一日APT，終生APT


Suspicious URL:: 母親節巷弄轉角違規停車 - 郵件 (HTML)
檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)
中華電信設備維護公告 - 郵件 (HTML)
高速公路通行費收費標準-103年開始全面實施 - 郵件 (HTML)
回覆(R) 全部回覆(L) 轉寄(W)
寄件者: 市政信箱確認函 [tpifd101@mail.taipei.gov.tw]
寄件日期: 2016/5/24 (週二) 上午 10:20
收件者:
副本:
主旨: 1050520巷弄轉角違規停車
訊息 1050520違規停車通知單.doc
親愛的網路市民，您好
本確認信函為系統自動寄發之確認信函，不要針對此郵件直接回覆。
[*] 請務必點選附檔以完成案件之確認。
[*] 如無法正常顯示，請啟用巨集功能。
[*] 請牢記[案號]與[密碼]以利後續之查詢。
案號：10505203665
密碼：tpE3665
查詢網址： http://i.taipei.gov.tw/web/guest/
台北市政府停車管理工程處 敬上

為什麼防不勝防?

缺乏防護意識

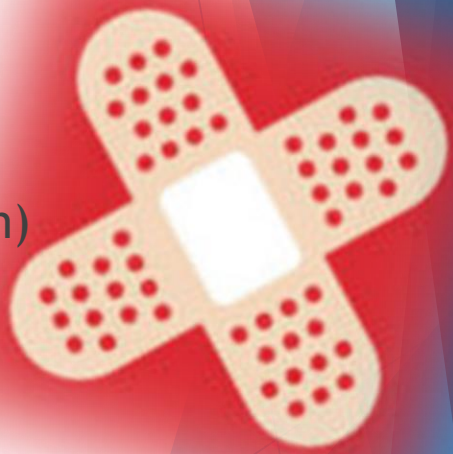
程式修補的延遲

- 超過99%的漏洞(exploited vulnerabilities)再被公布一年後仍被駭客使用來進行攻擊。
  - 76% 被利用來攻擊的漏洞是超過兩年的。
    - 9%被利用來攻擊的漏洞已超過十年!!!

缺乏應變機制

- 74% 的組織沒有正式的事件應變計畫(incident response plan)

- 沒有漏洞管理計畫(vulnerability management program)的組織需花近200天方能修補其系統

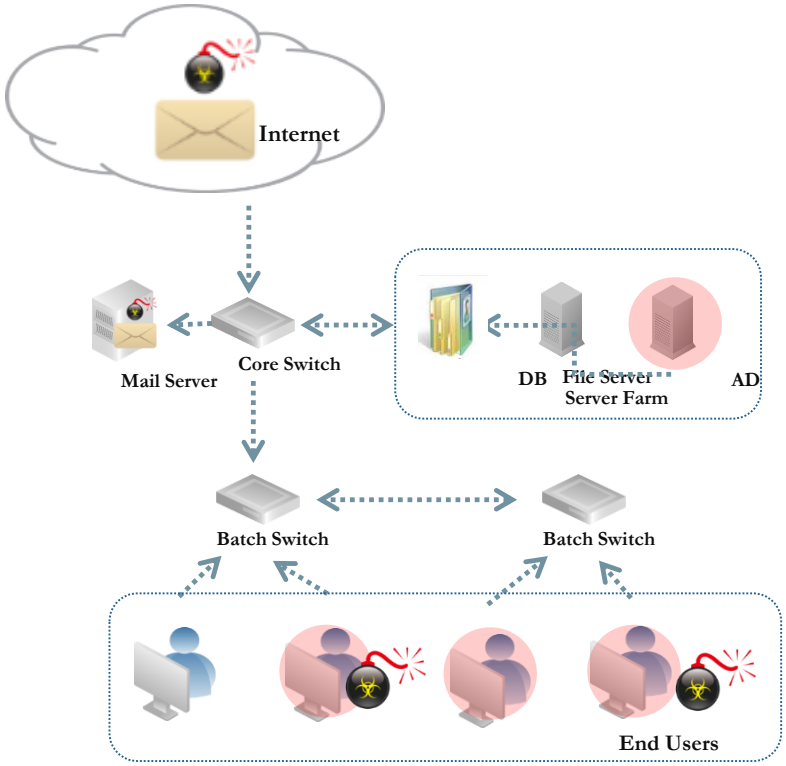


APT 防禦的現況與挑戰(Cont)

Questions	Problems
定位出的受害電腦是否準確? 會不會有誤判或遺漏?	單一sensor/rule的資訊不足以佐證確切的駭客行為(駭客慣用正常行為入侵)。
此駭客入侵事件僅止於此嗎? 有其他受害者嗎? 影響範圍有多大?	缺乏足夠的駭客行為情資，無法進行跨產品資安事件紀錄之關聯性分析。
如何處理此受害電腦? 有什麼資料被竊? 駭客是如何入侵此電腦的?	缺乏電腦詳細記錄檔及歷史資料，無法追蹤受害當時的駭客行為及軌跡。

即便收集各式資料，要如何儲存、處理、並有效快速的關聯分析?

目標式持續威脅攻擊示意圖



1. 惡意郵件投遞到企業郵件主機
2. 用惡意文件攻擊端點程式弱點
3. 控制某些端點後進行內部擴散
4. 透過端點攻擊AD擷取密碼資料
5. 駭客利用停用的帳號或是建立最高權限帳號
6. 用合法帳號存取DB或檔案主機
7. 打包資料並帶走

判斷釣魚信件的五個細節

一、標題：

此封信件的標題為「登入告警：嘗試登入達到認證上限」，其中「登入告警」很明顯為中國用語，在繁體中文的環境下，正常應會被寫作「登入警告」，而不會使用「告警」。

二、寄件者：

為避免冒用，Google 不會使用 gmail.com 結尾的電子信箱來寄送任何 Google 系統信件，因為 Gmail.com 任何人都能註冊，這封信件結尾卻使用了 gmail.com。

三、信件內容：

信件內圖片網址的持有者不是 Google ， 然而，Google 系統通知信內附的圖片不使用 Google 旗下的伺服器或網站，即是一個非常可疑的疑點。

四、連結或者附件內容：

雖然頁面長的跟 Google 登入畫面一模一樣，但要求帳戶安全檢查等連結網址的持有人卻不是 Google。

五、交叉確認：

Google 帳戶安全警告除了利用 Email 通知外，Google 通常會另行顯示在帳戶內的其他地方，例如會顯示在我的帳戶 → 裝置活動與通知 → 近期安全事件。使用者可以利用這個功能確認 email 所描述的安全事件是否真的存在。

平時對 Gmail 帳號的資安維護

一、打開 Google 兩階段驗證：

設定帳戶兩階段驗證完成，使用者輸入登入帳戶密碼之後，系統會透過簡訊或其他方式寄送驗證碼到使用者的行動裝置上，或是透過 app 自動產生驗證碼，使用者需要再次輸入收到的驗證碼才能完成登入。此驗證方法的目的在於利用使用者的行動裝置再次確認登入者的身分，多一個確認步驟，增加駭客入侵的難度。

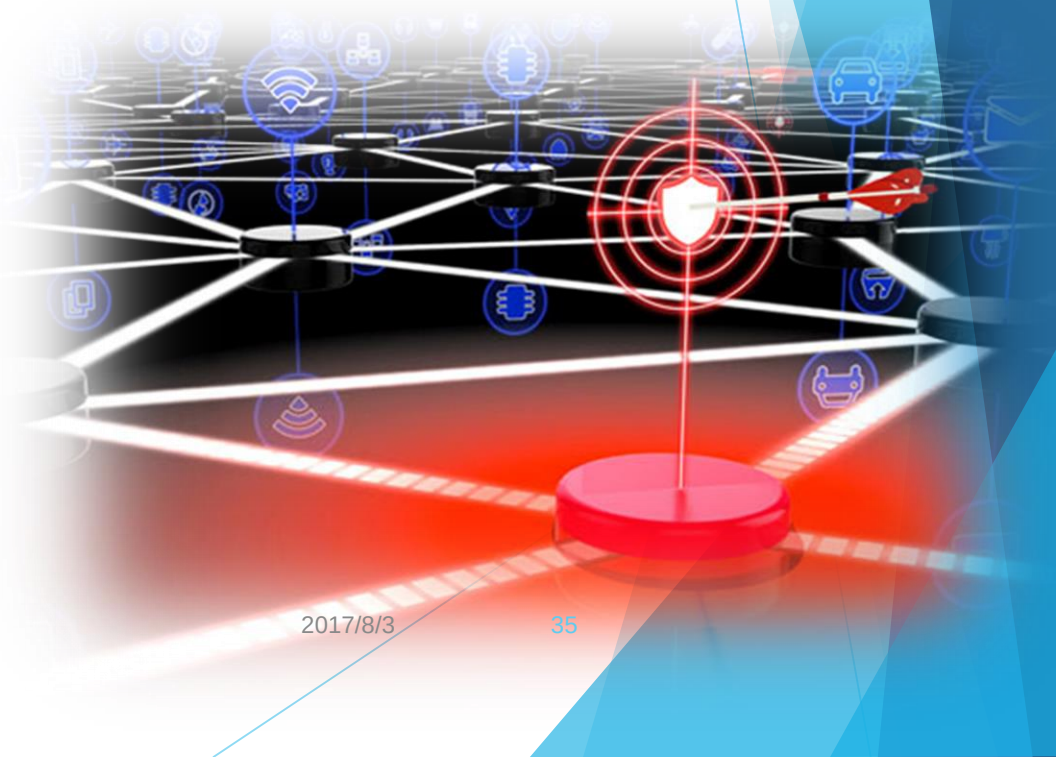
二、從 Google 研究功能中打開 Gmail 的驗證功能：

啟用 Gmail 驗證功能後，Gmail 會在寄件者地址旁邊提示使用者是否通過身分認證，開啟此功能後，真正的 Google 系統郵件旁邊會額外顯示鑰匙圖示。

> 不要以為自己沒有什麼重要的資訊就不會被入侵，你可能會變成有意人士攻擊別人的節點。

小結

- 因應APT的第一步也是最重要的一步就是”對APT正確的觀念與認知”。
- 對抗APT沒有特效藥，須結合適當的政策、流程以及人員配置及訓練，加上外部技術與服務以建立防禦的策略與戰術。
- 簡言之，APT防禦就是引進防禦技術及落實資安治理。

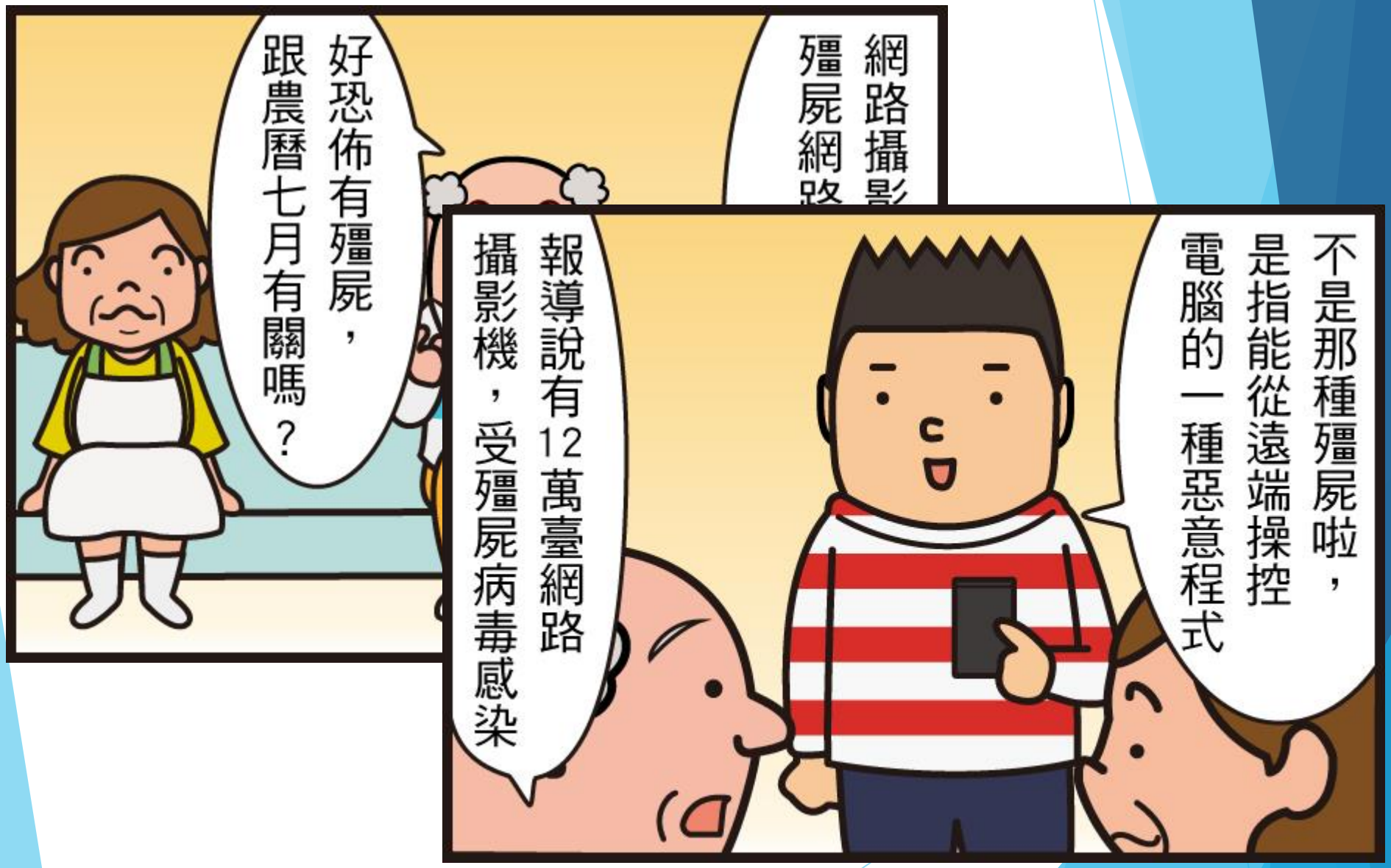


Agenda

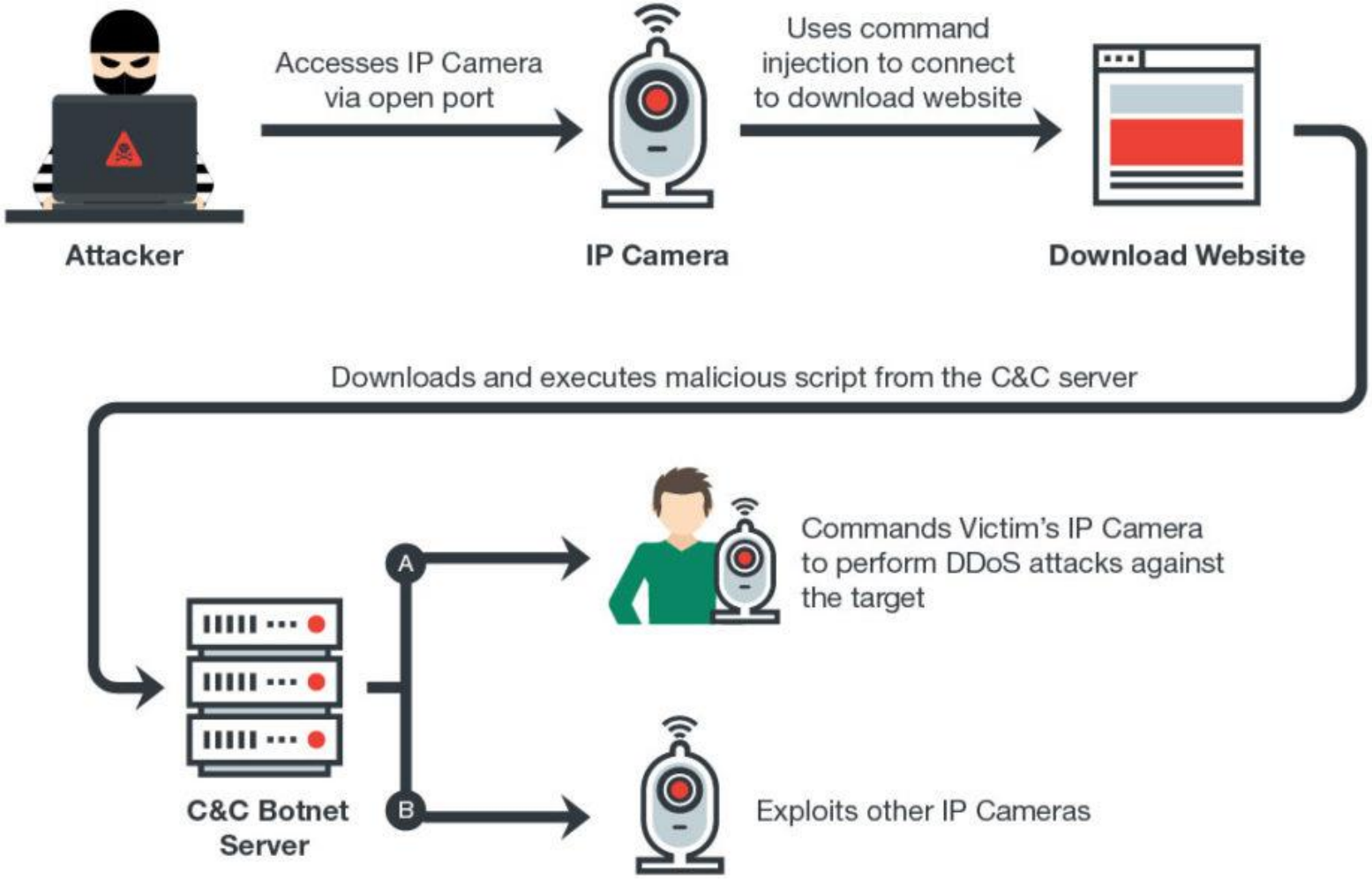
- 引言
- 資安威脅趨勢
  - 資料外洩助長攻擊和勒索
  - 潛藏的禍害
  - 未來的隱憂 - IOT Security
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

未來的隱憂 - IOT Security

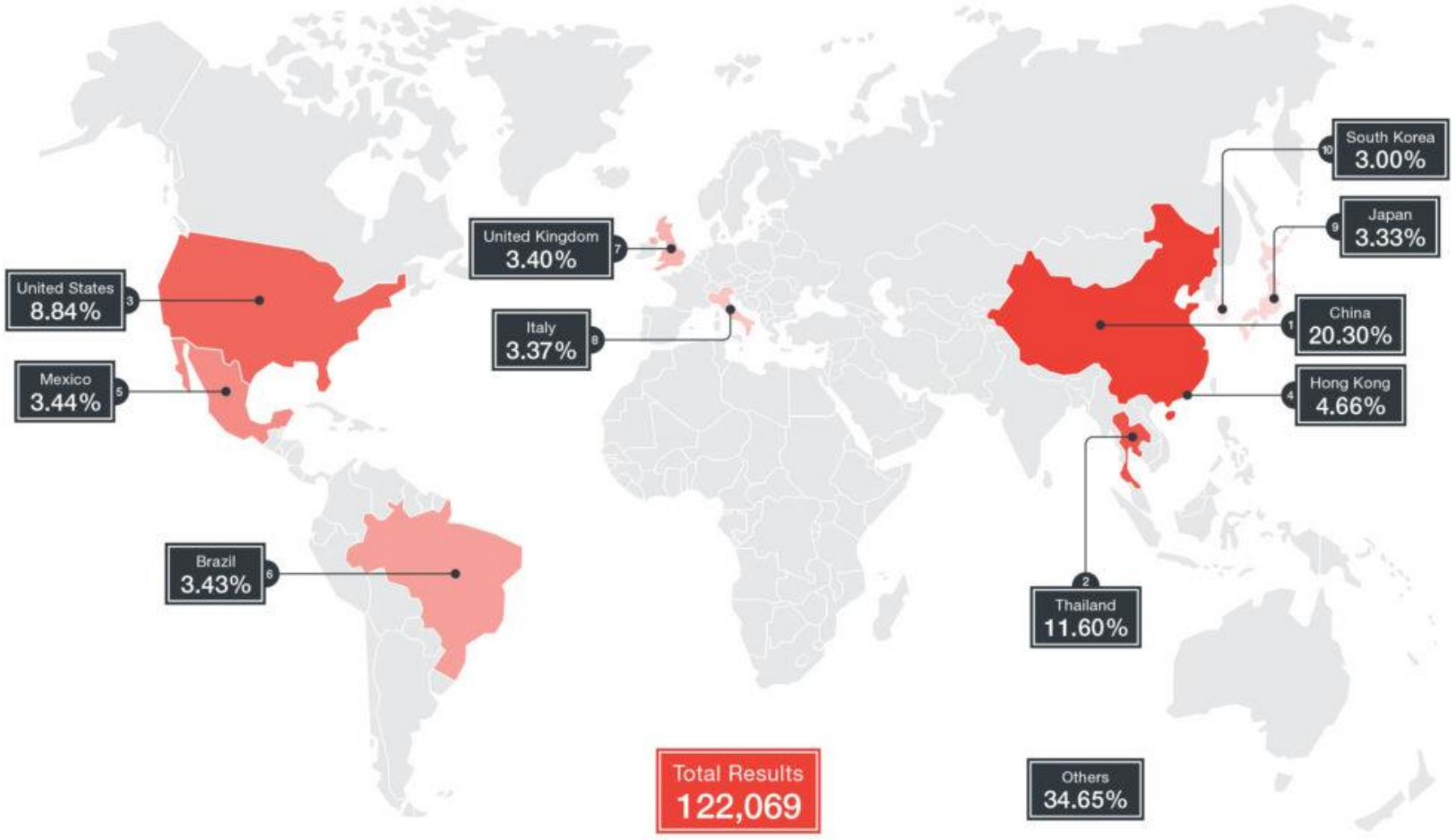
It's Happening – Around You


網路攝影
殭屍網路
好恐佈有殭屍，
跟農曆七月有關嗎？
報導說有12萬臺網路
攝影機，受殭屍病毒感染
不是那種殭屍啦，
是指能從遠端操控
電腦的一種惡意程式

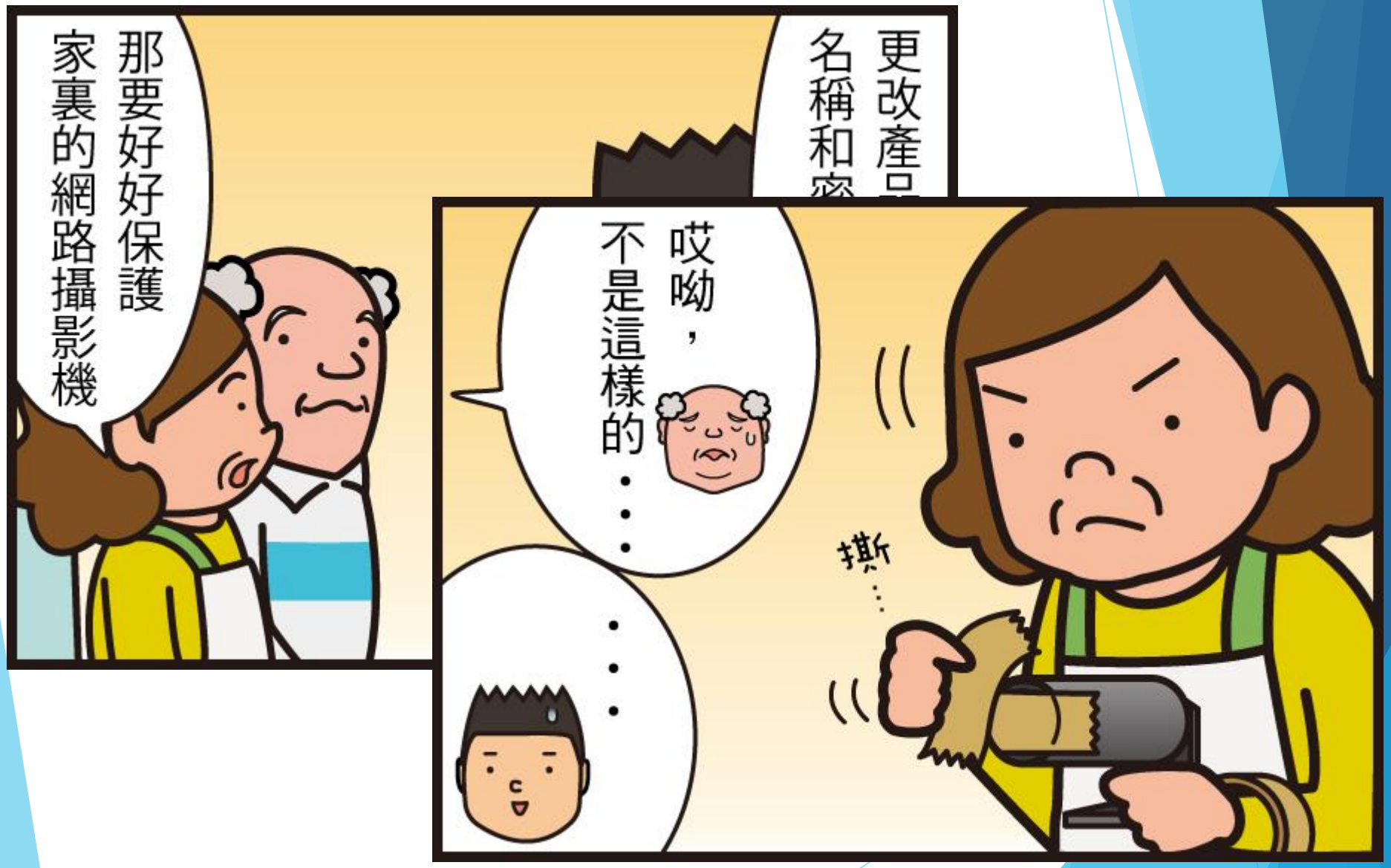
殭屍病毒Persirai感染網路攝影機



多達1,000多種型號,12萬臺網路攝影機,恐受感染



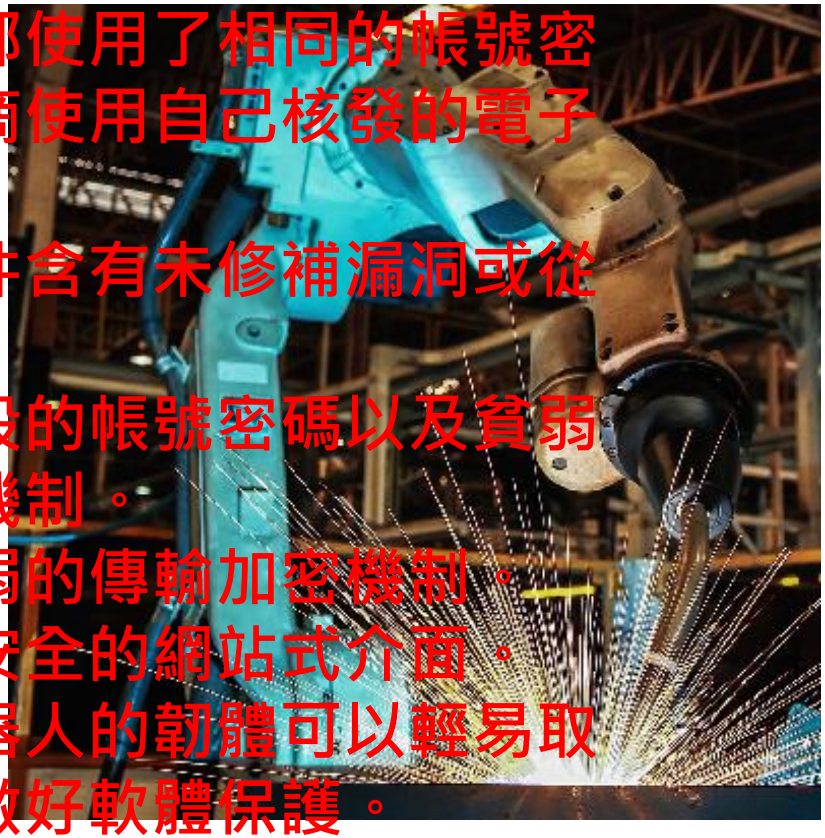
到2017年4月26日為止可被入侵的網路攝影機數量（資料來自Shodan）


更改產品
名稱和密
哎呦，
不是這樣的……
……
撕……
那要好好保護
家裏的網路攝影機

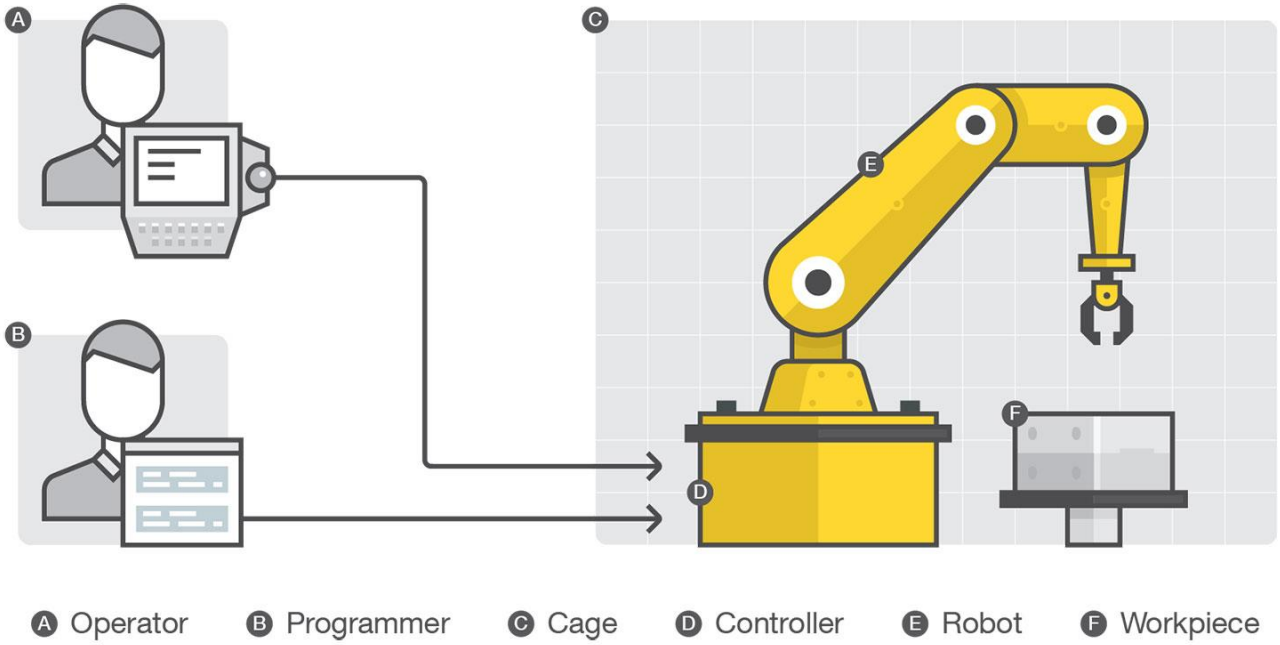
智慧型家電,監控攝影機... 等，永遠變磚塊

工業4.0智慧工廠浪潮正夯 工業機器人恐成駭客箭靶

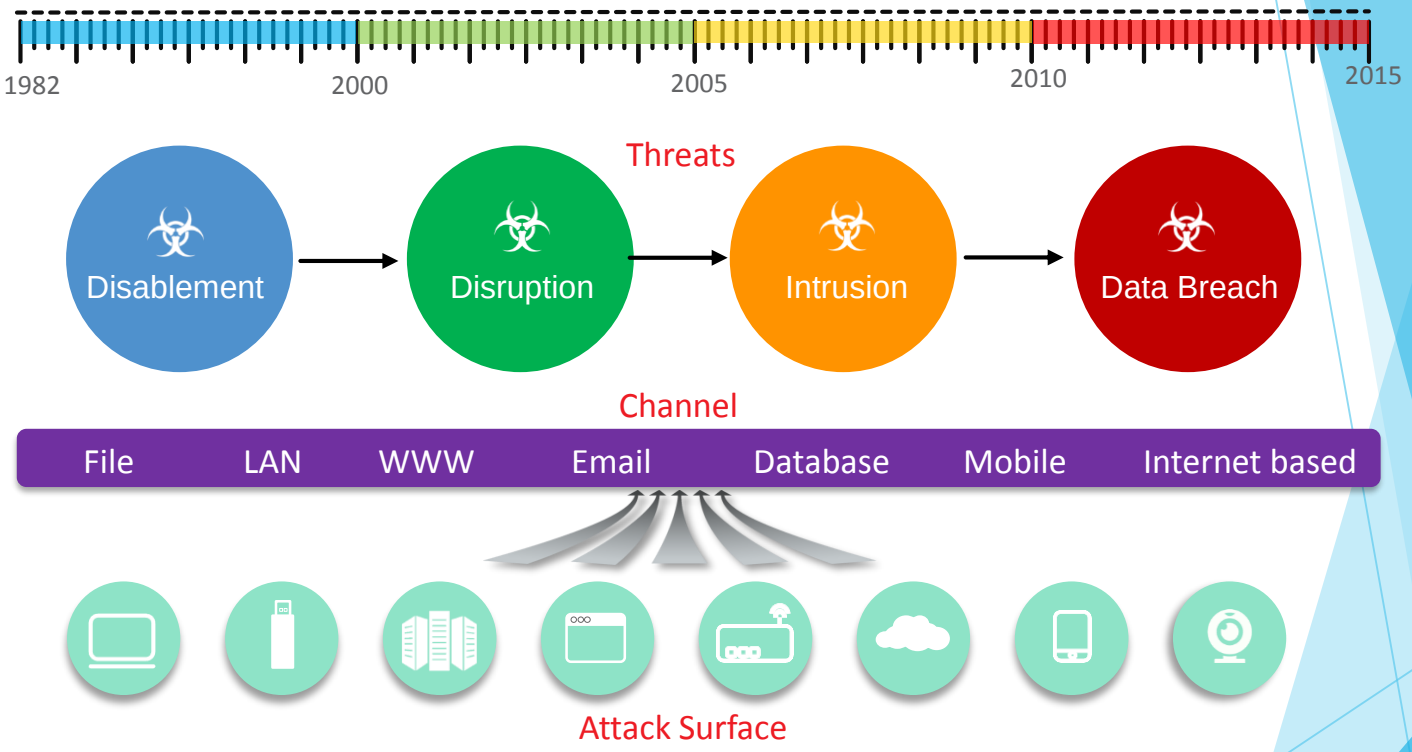
- 廠商在公開網站上提供了詳細的技術文件、廠商在每一台機器人上都使用了相同的帳號密碼、廠商使用自己核發的電子簽章。
- 軟體元件含有未修補漏洞或從未更新。
- 使用預設的帳號密碼以及貧弱的驗證機制。
- 使用貧弱的傳輸加密機制。
- 使用不安全的網站式介面。
- 廠商機器人的韌體可以輕易取得，未做好軟體保護。



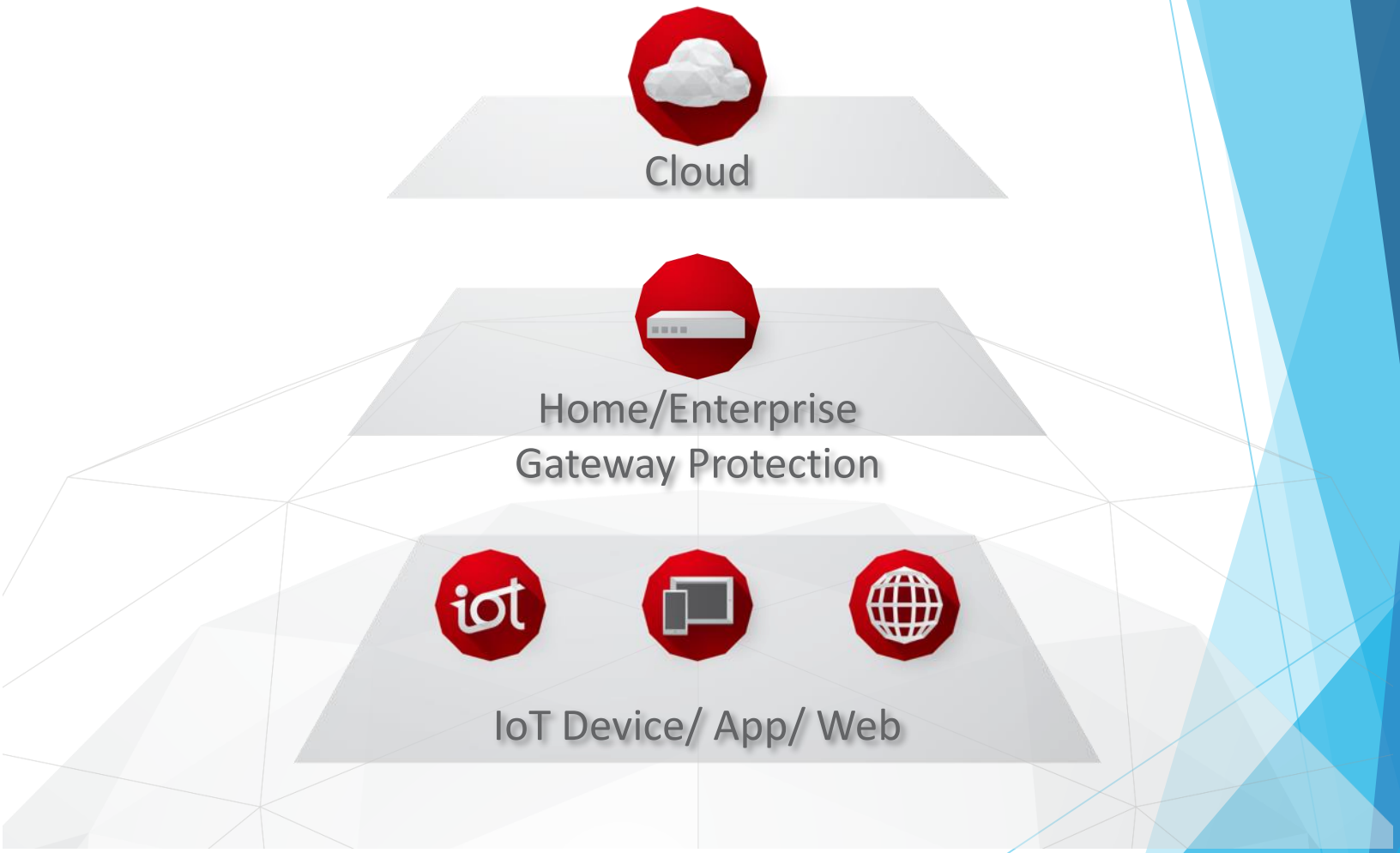
機器人可能遭到什麼樣的攻擊？



IoT World – More attack surfaces for hackers



Full Range IoT Security Solution Overview



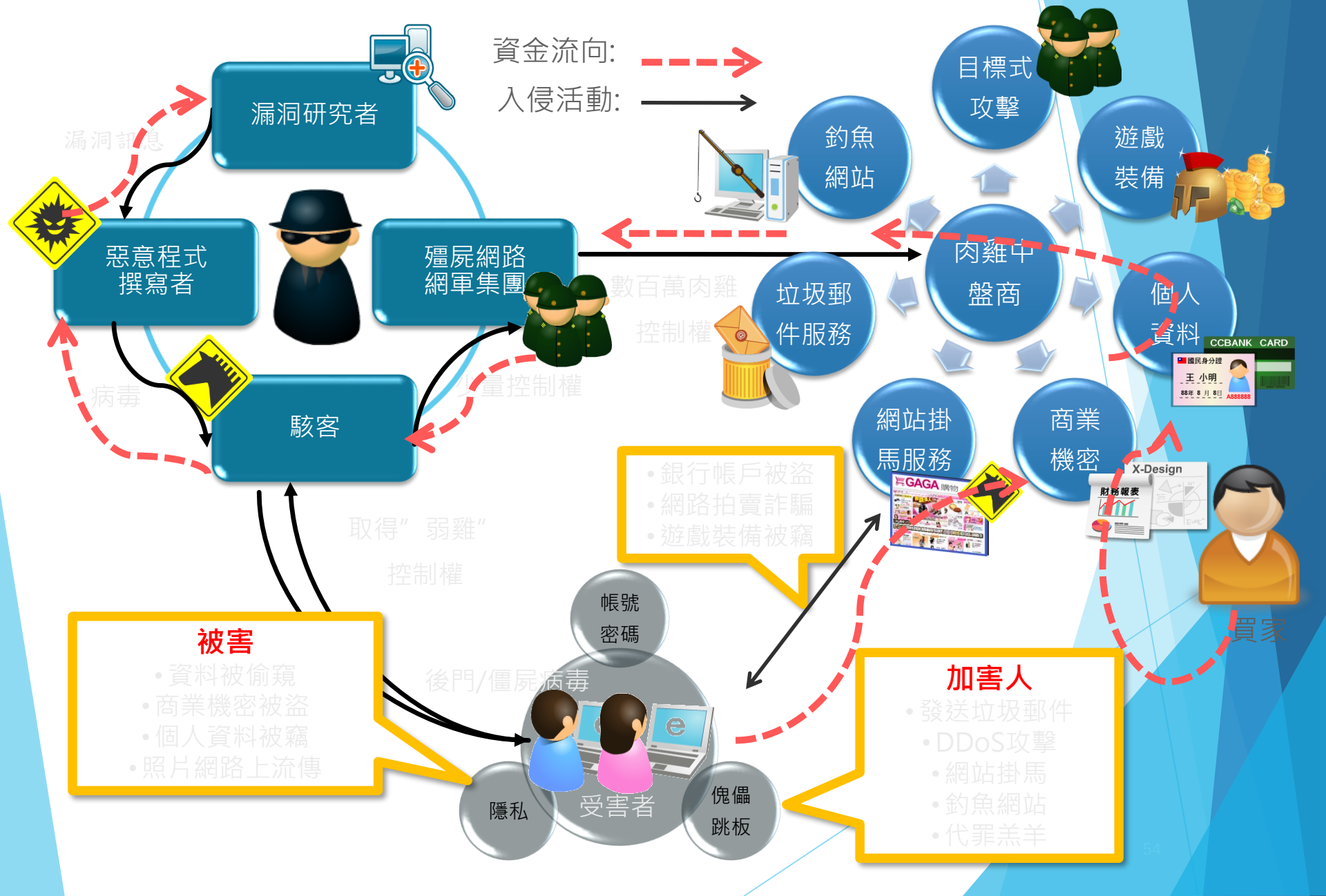
如何預防與因應

- 盡可能避免所有工業控制系統 (ICS) 裝置連上對外網路/網際網路。
- 啟用防火牆並且將 ICS 裝置與企業網路隔離。
- 當從遠端存取 ICS 裝置時，務必透過虛擬私人網路 (VPN)。
- 定期更新/修補系統，一有更新便立即套用。
- 增加額外的驗證機制，特別是針對系統管理員帳號。

Agenda

- 引言
- 資安威脅趨勢
  - 資料外洩助長攻擊和勒索
  - 潛藏的禍害
  - 未來的隱憂 II
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

黑色產業鏈


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

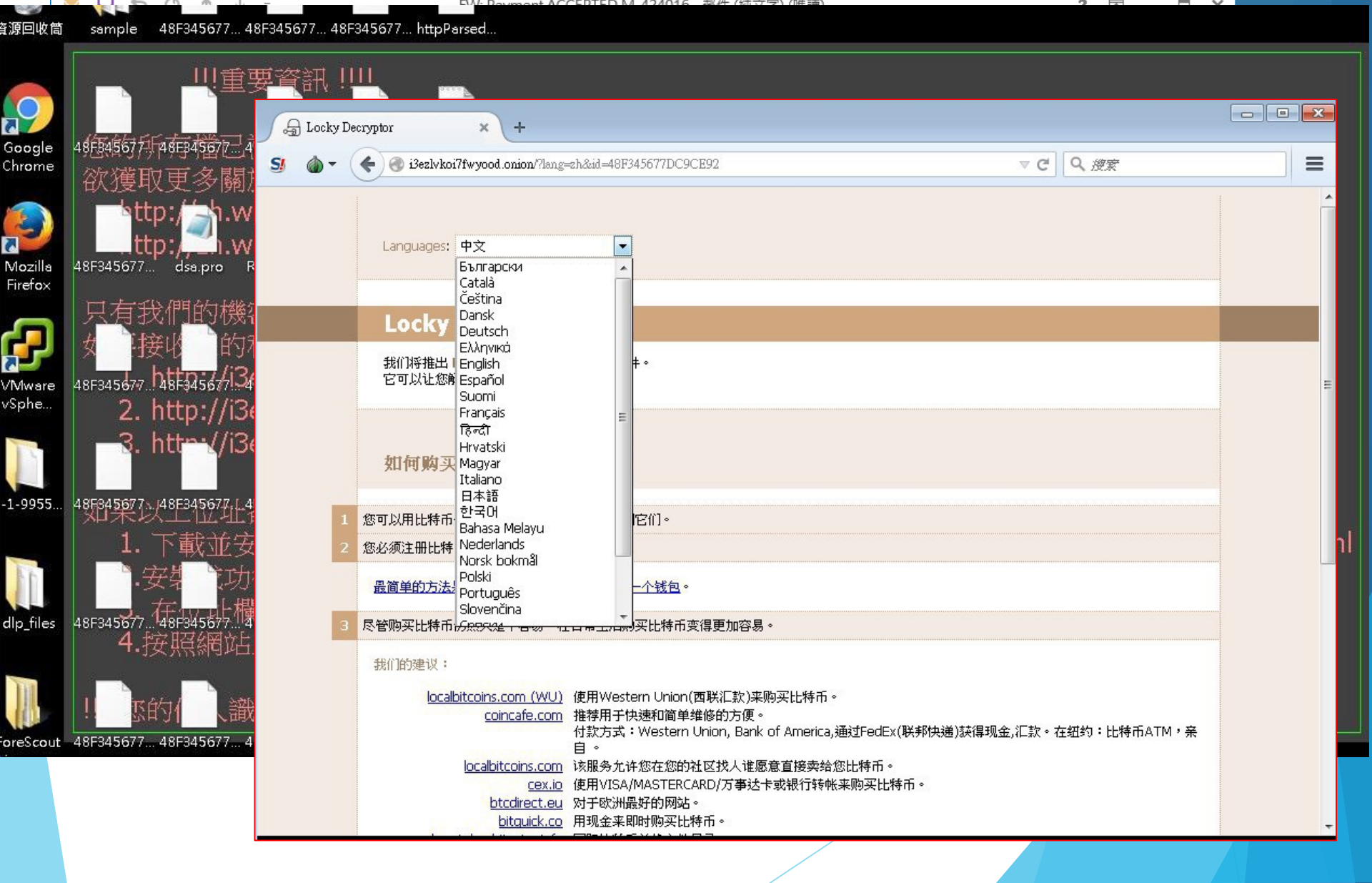
未來資安預測

- **整體資安威脅趨勢正朝向「個人化」發展**
  - 對於網路犯罪集團如何不斷發揮創意來攻擊一些意想不到的目標，過去已經有很多討論。然而過去這一年，卻證明了網路犯罪集團其實不需最先進的技術或精密的手法就能得逞。有時候，歹徒只需掌握每一種手法背後的受害者心理，就能彌補技術上的不足。
- **威脅個人或企業名譽的攻擊**
  - 網路勒索集團將會想出更多新的方法來針對個別受害者的心理，讓每一次的攻擊變得更「個人化」，不論其目標是特定使用者或是某家企業。名譽就是一切，因此能夠威脅個人或企業名譽的攻擊，不但非常有效，而且最重要的，非常有利可圖。
- 智慧**連網家用裝置的不斷成長**，將促使網路駭客**利用一些未修補的漏洞**來發動一場全面性攻擊。
- 在行動領域，新一代支付機制將吸引歹徒的覬覦，進而**將目標從 EMV 信用卡移轉至行動錢包**，屆時這類號稱「更安全」的支付平台將受到嚴格考驗。

Agenda

- 引言
- 資安威脅趨勢
- 網路勒索之年
  - 恐嚇取財手法十年進化史
  - 勒索軟體感染途徑與特性
  - 即時處置
- 案例分享
- 如何因應與面對
- Q&A

https://youtu.be/Sm5TbBKeFvU



2006年:起源

惡意程式特性	描述
偵測命名	TROJ_CRYPZIP.A
加密技術	密碼
加密原則	特定副檔名
加密方式	使用密碼壓縮檔案 並刪除原始檔案
付款金額	300 USD
解決方式	DLL內暗藏密碼

2011年:實驗摸索階段

惡意程式特性	描述
偵測命名	TROJ_RANSOM.QOW
加密技術	系統鎖定
加密原則	特定副檔名
加密方式	使用密碼壓縮檔案並刪除原始檔案
付款金額	12 USD
解決方式	付費電話
估計獲利	30,000 USD

2012年:青春期-血氣方剛的恐嚇伎倆

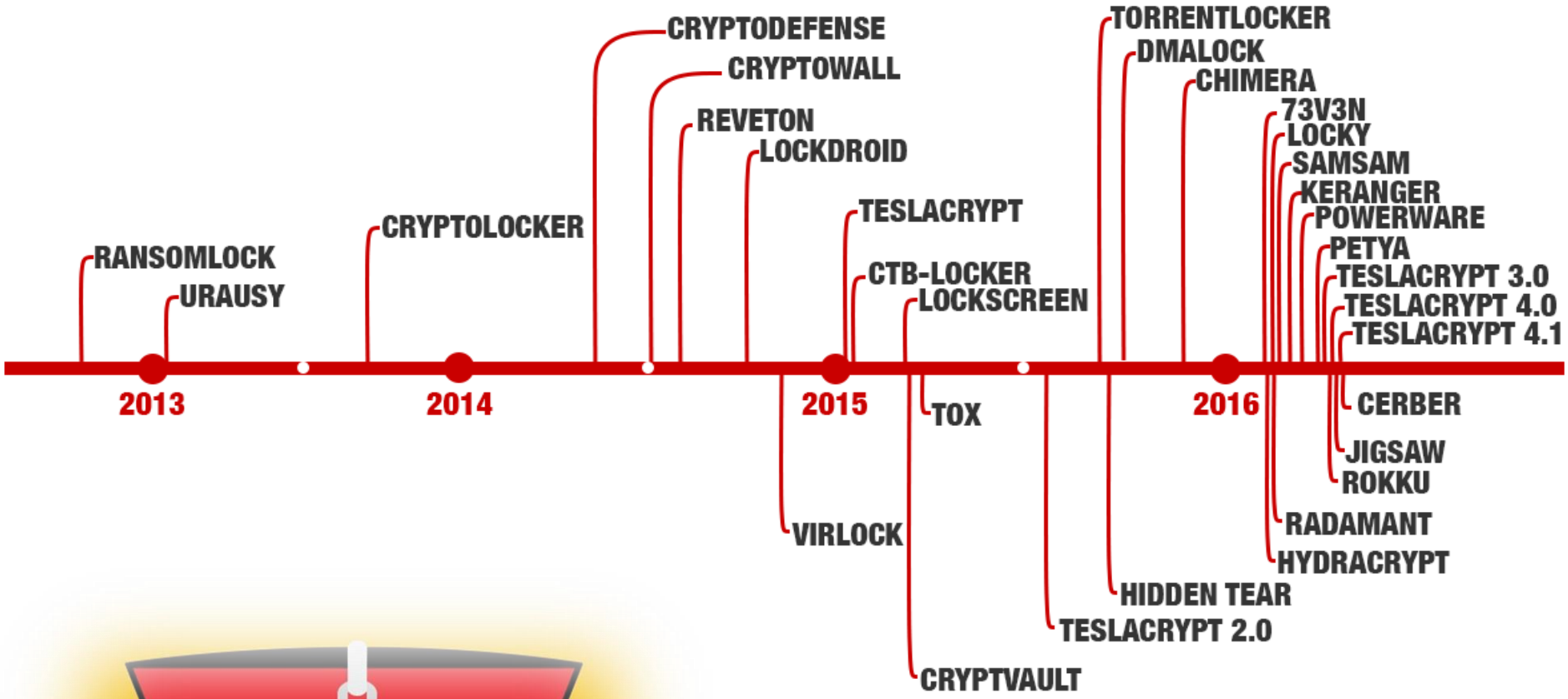
惡意程式特性	描述
偵測命名	REVETON
加密技術	金鑰
加密原則	特定副檔名
加密方式	檔案加密、系統鎖定
付款金額	300 USD
解決方式	付費電話
估計獲利	N/A

2013年:更爐火純青的加密手法

惡意程式特性	描述
偵測命名	Cryptolocker
加密技術	金鑰
加密原則	特定副檔名
加密方式	二層式加密技術 (AES & RSA)
付款金額	300 USD
解決方式	付費電話
估計獲利	N/A

2014-2015年:更多元的支付方式

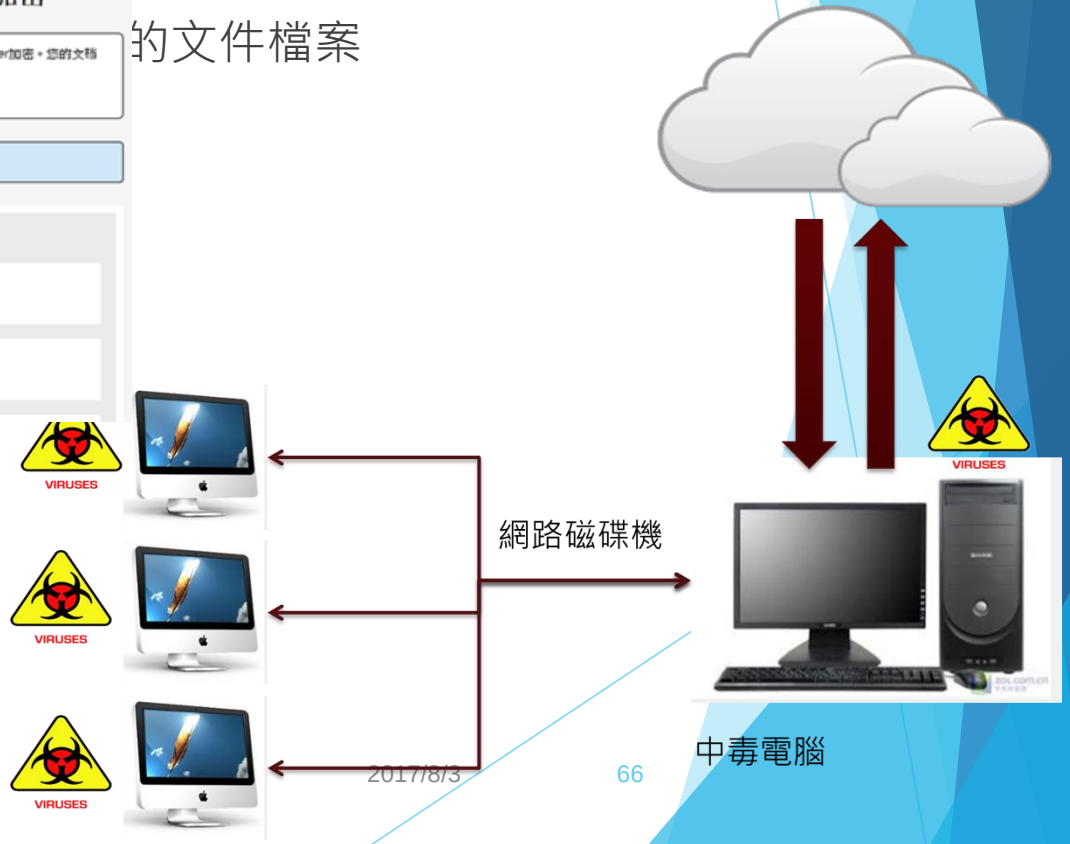
惡意程式特性	描述
偵測命名	TROJ_CRYPTRBIT.H
加密技術	金鑰
加密原則	特定副檔名
加密方式	二層式加密技術 (AES & RSA)
付款金額	300 USD
解決方式	比特幣
估計獲利	N/A


RANSOMLOCK
URAUSY
CRYPTOLOCKER
CRYPTODEFENSE
CRYPTOWALL
REVETON
LOCKDROID
TESLACRYPT
CTB-LOCKER
LOCKSCREEN
TORRENTLOCKER
DMALOCK
CHIMERA
73V3N
LOCKY
SAMSAM
KERANGER
POWERWARE
PETYA
TESLACRYPT 3.0
TESLACRYPT 4.0
TESLACRYPT 4.1
2013
2014
2015
2016
CERBER
JIGSAW
ROKKU
TOX
VIRLOCK
RADAMANT
HYDRACRYPT
HIDDEN TEAR
TESLACRYPT 2.0
CRYPTVAULT

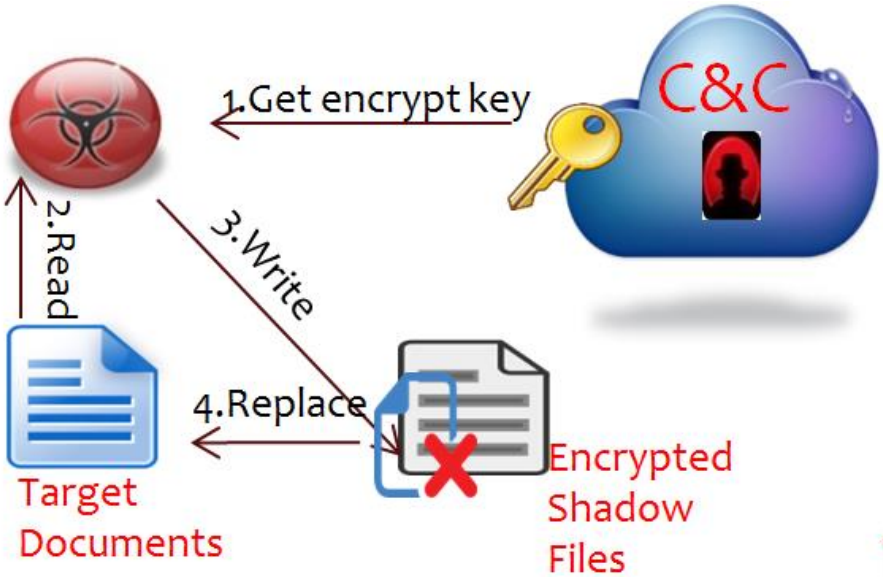
勒索軟體的特性(1)：把你的檔案當作人質“加密”

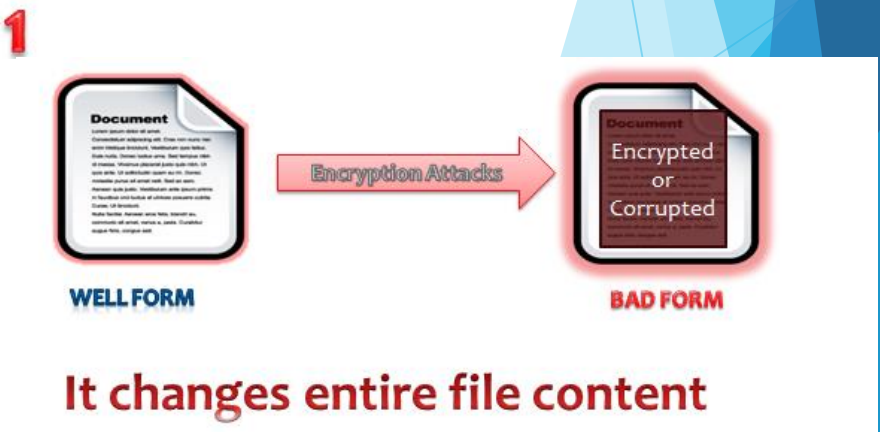
檔案

的文件檔案



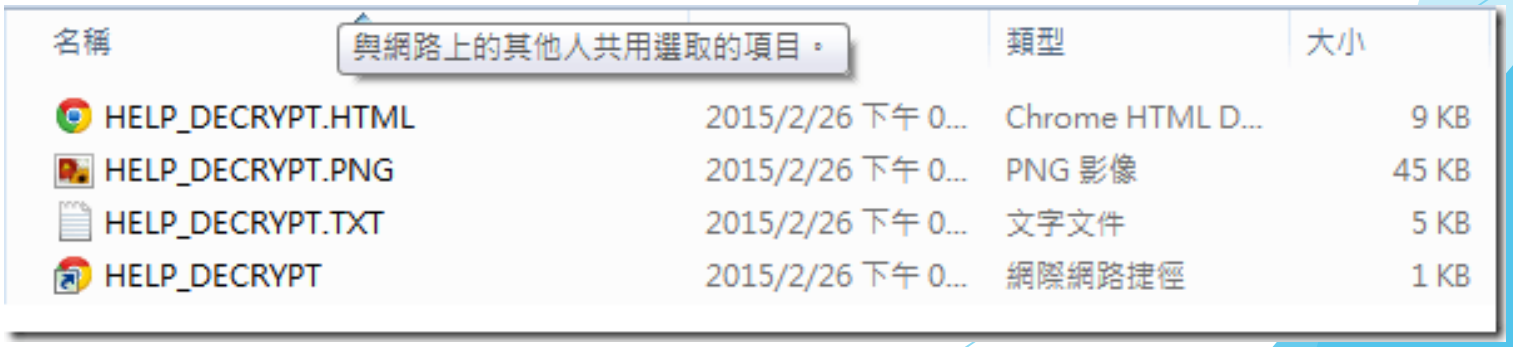
勒索軟體的特性(2)：文件無法自行解密





勒索軟體的特性(3) ：被加密文件將無法使用

- 中了此類病毒後會優先攻擊文件、圖片、影音資料被加密，文件檔案會多一串 「encrypted、exx 、 micro、mp3 ……」的字眼
- 所有被加密檔案將無法使用



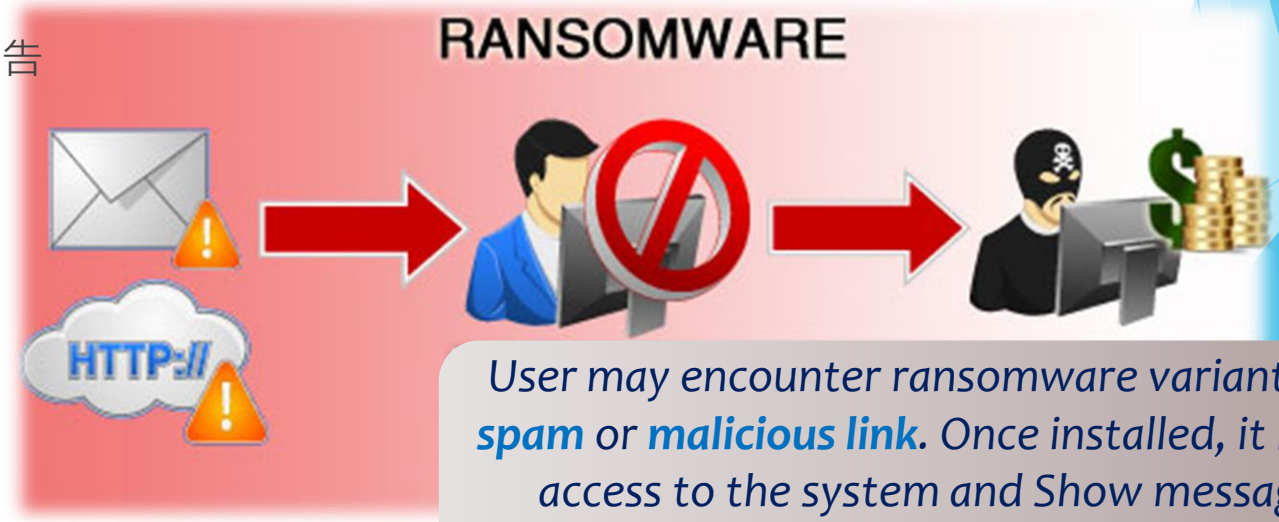
勒索軟體的特性(4) ：勒索付錢才給解密鑰匙

- 彈跳出勒索畫面要求支付贖金

勒索軟體的散播途徑

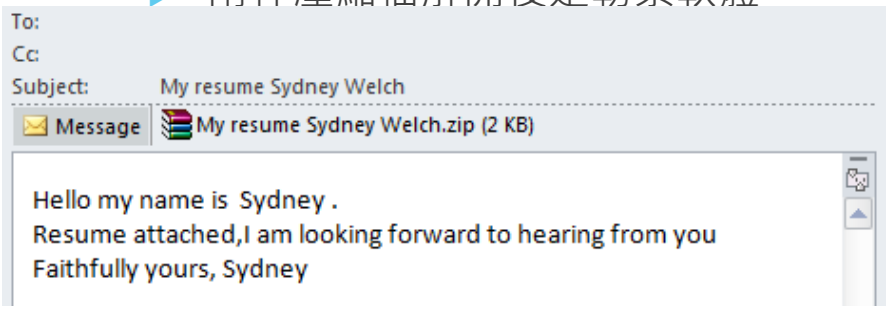
勒索軟體目前主要的攻擊途徑:

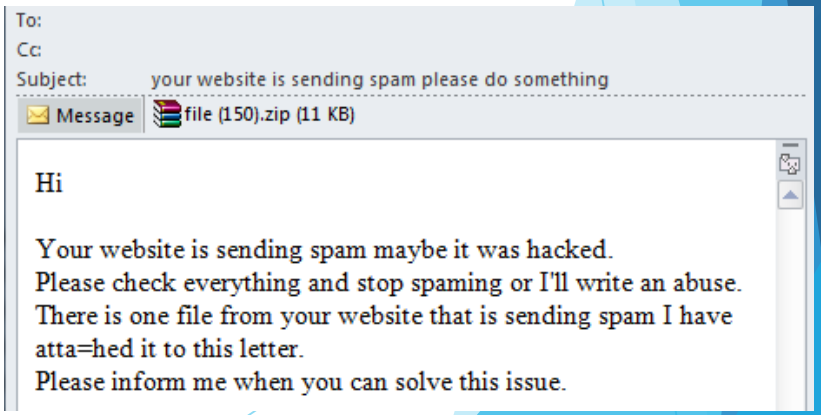
- 惡意郵件
  - 釣魚連結和惡意夾檔
- 網頁掛馬
  - 遭駭客入侵的網站
  - 惡意廣告



惡意郵件攻擊案例

- 釣魚信件
  - 假冒當地的銀行或快遞，連結下載帳單或
  - 下載的檔案實際為勒索軟體
- 惡意夾檔
  - 偽裝成投履歷或寄送發票的信件
  - 附件壓縮檔解開後是勒索軟體





RTLO手法

ooo企劃cod.scr ← 真正的檔案名稱

ooo企劃[U+RTLO]cod.scr Unicode控制符號 →由右至左顯示

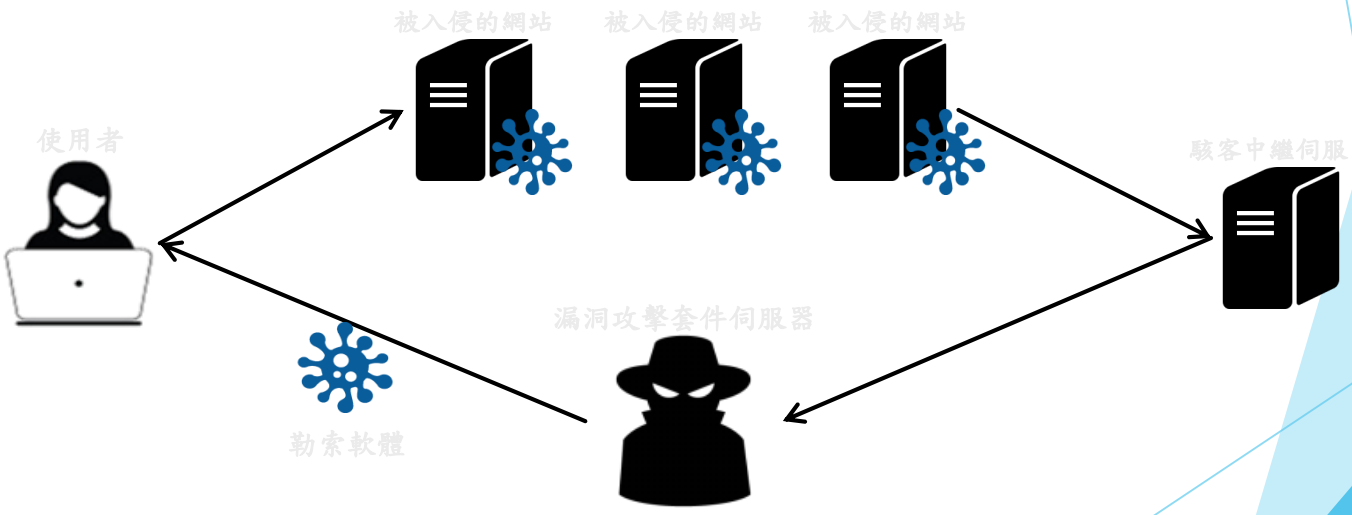
ooo企劃rcs.doc ← 顯示出來給你看到的檔案名稱

網頁掛馬攻擊統計

- 從2015年十月開始在台灣劇烈活動
- 第四季的攻擊總數有3.5倍的成長
- 從Q3的43,015次至Q4的152,929次

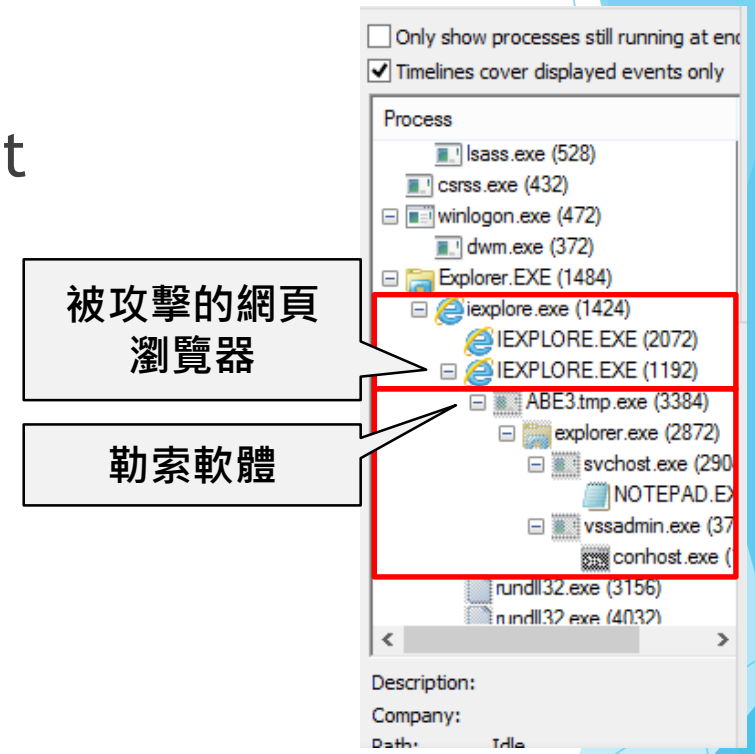
網頁掛馬攻擊流程

- 駭客入侵網站後，將惡意程式碼植入網站
- 拜訪該網站的使用者將會執行程式碼
- 在瀏覽網站的同時，也自動被導入駭客的攻擊伺服器



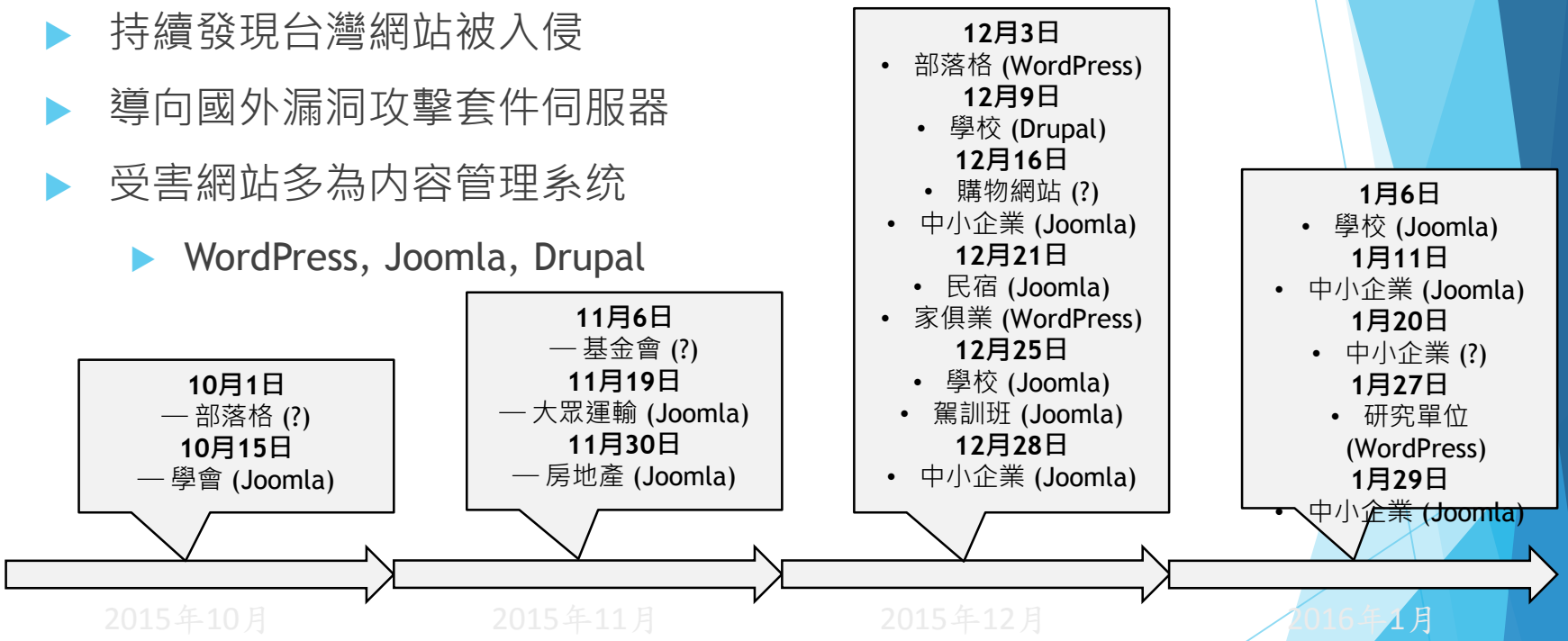
網頁掛馬攻擊行為分析

- 惡意連結從遠端下載Exploit
- 攻擊應用程式漏洞
  - 網頁瀏覽器 (如IE)
  - 瀏覽器外掛 (如Flash)
- 攻擊成功後
  - 取得應用程式控制權
  - 自動下載並執行勒索軟體



台灣網站掛馬攻擊 追蹤發現

- 持續發現台灣網站被入侵
- 導向國外漏洞攻擊套件伺服器
- 受害網站多為內容管理系統
  - WordPress, Joomla, Drupal



漏洞攻擊套件 (Exploit Kit)

Simple browser statistics

Browser	Visits	Exploited	Percent
MSIE	10032	526	5.24%
Firefox	2402	175	7.29%
Other	4872	134	2.75%
Opera	322	15	4.66%

Main Statistics

Unique Visits	Exploited	Percent
17628	850	4.82%

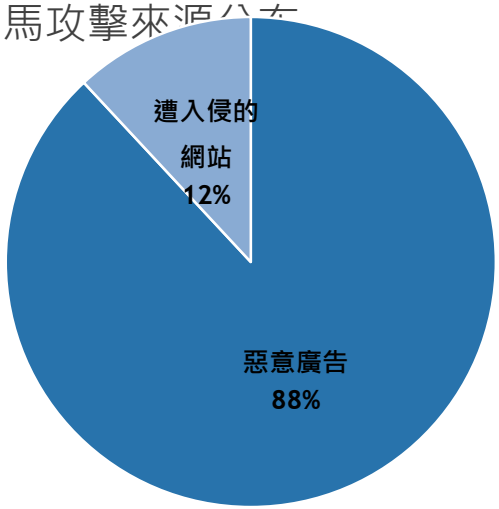
Exploit statistics

Exploit	Exploited	Percent
JAVA TC	278	1.58%
JAVA SMB	187	1.06%
HCP	28	0.16%
PDF COLLAB	72	0.41%
PDF PRINTF	8	0.05%
FLASH 9	9	0.05%
PDF LIBTIFF	209	1.19%
IEPEERS	15	0.09%
MDAC	44	0.25%

- 主要為網站伺服器形式
  - 包含多種Exploit
  - 提供使用者上傳病毒進行散播
  - 具有多種避免偵測的功能
  - 管理者統計功能
- 攻擊套件伺服器的拜訪者將被攻擊
  - 攻擊者只需要考慮如何誘導使用者
- 2015年有五種以上主流的漏洞攻擊套件
  - Angler, Magnitude, Nuclear, Neutrino, Rig

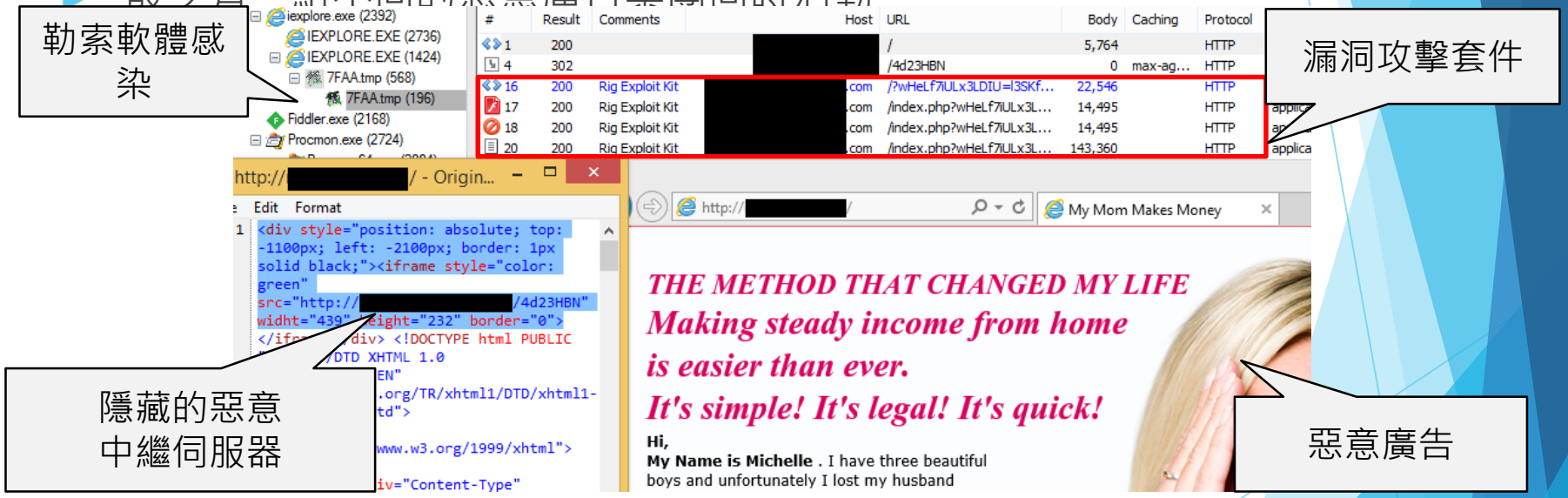
萬惡深淵: 廣告進行掛馬攻擊

- 惡意廣告與掛馬攻擊
  - 駭客假冒廣告業主，上傳惡意廣告到一般廣告平台
  - 惡意廣告可透過廣告網路傳遞到各大網站
  - 2015年12月全球網頁掛馬攻擊來源分布



台灣的廣告攻擊案例

- 主要是被全球性的惡意廣告波及
- 最少有三組不同的惡意廣告集團同時活動



為什麼駭客選擇惡意廣告

- 廣告網路複雜
  - 難以察覺和追蹤 (廣告可依照地區、時間、喜好來推播)
- 廣告未被檢驗
  - 大部分廣告平台沒有能力驗證廣告是否具有攻擊性
  - 多層的上下游關係難以驗證
- 更容易進行大量攻擊
  - 廣告可以播送到大型網站
  - 不需要使用者點擊

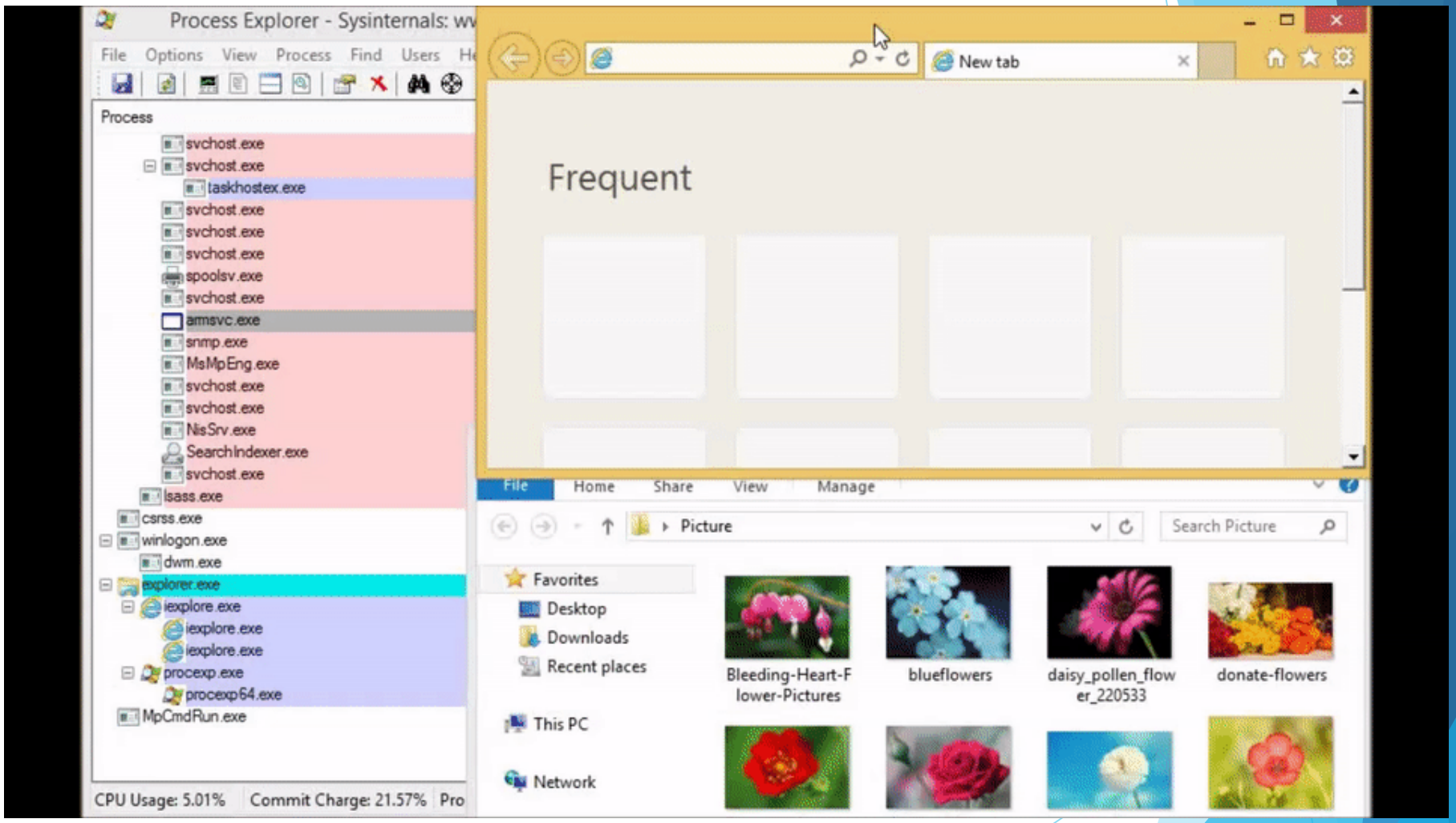
駭客攻擊奏效的關鍵

- 持續發現新漏洞是主
  - 零時差漏洞
  - 快速整合漏洞

越久沒有更新
感染風險越高

CVE 編號	應用程式	發現日期	整合的漏洞攻擊包	更新公開日期	差距天數
CVE-2016-0034	MS Silverlight	2016-02-22	Angler Exploit Kit	2016-01-12	41
CVE-2015-8651	Adobe Flash	2016-01-26	Angler Exploit Kit	2015-12-28	29
CVE-2015-8446	Adobe Flash	2015-12-15	Angler Exploit Kit	2015-12-08	7
CVE-2015-7645	Adobe Flash	2015-10-29	Angler Exploit Kit	2015-10-16	13
CVE-2015-5560	Adobe Flash	2015-08-28	Angler Exploit Kit	2015-08-11	17
CVE-2015-2444	MS IE	2015-08-25	Sundown Exploit Kit	2015-08-12	13
CVE-2015-2419	MS IE	2015-08-10	Angler Exploit Kit	2015-07-22	19
CVE-2015-1671	MS Silverlight	2015-07-21	Angler Exploit Kit	2015-05-12	70
CVE-2015-5122	Adobe Flash	2015-07-11	Angler Exploit Kit	2015-07-14	-3
CVE-2015-5119	Adobe Flash	2015-07-07	Angler Exploit Kit	2015-07-08	-1
CVE-2015-3113	Adobe Flash	2015-06-27	Magnitude Exploit Kit	2015-06-23	4
CVE-2015-3104	Adobe Flash	2015-06-17	Angler Exploit Kit	2015-06-09	8
CVE-2015-3105	Adobe Flash	2015-06-16	Magnitude Exploit Kit	2015-06-09	7
CVE-2015-3090	Adobe Flash	2015-05-26	Angler Exploit Kit	2015-05-12	14
CVE-2015-0359	Adobe Flash	2015-04-18	Angler Exploit Kit	2015-04-14	4
CVE-2015-0336	Adobe Flash	2015-03-19	Nuclear Exploit Kit	2015-03-12	7
CVE-2015-0313	Adobe Flash	2015-02-02	HanJuan Exploit Kit	2015-02-04	-2
CVE-2015-0311	Adobe Flash	2015-01-20	Angler Exploit Kit	2015-01-27	-7
CVE-2015-0310	Adobe Flash	2015-01-15	Angler Exploit Kit	2015-01-22	-7

勒索軟體行為 Live Demo
當你進入了被掛馬的網站



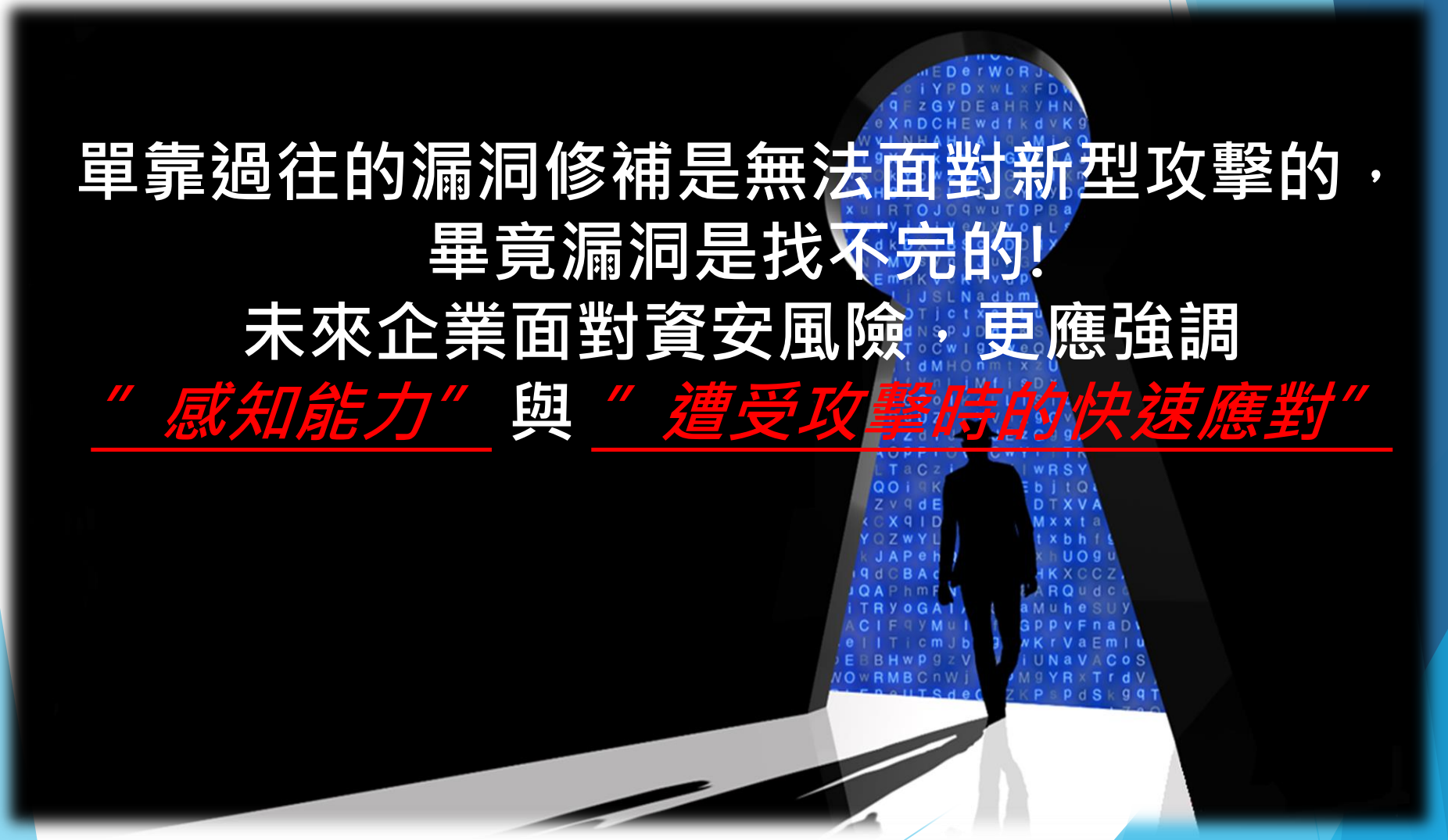
- 勒索軟體的崛起
  - 有效的犯罪手法，為地下經濟帶入新的金錢收入
  - 相關的犯罪隨之而起，更多的惡意廣告、惡意郵件和漏洞
- 勒索軟體的散播途徑
  - 惡意信件
  - 被駭客入侵的網站
  - 網路廣告
- 勒索軟體擴散的關鍵
  - **收件者沒有警覺，網站沒有更新，廣告難以驗證，軟體含有漏洞**


你的檔案已經被加密!!限期4天依指示付費,否則銷毀解鎖密碼
4
勒索軟體大舉入侵臺灣
至少20家臺灣企業受駭
Money!!
加密受害者檔案，甚至整個硬碟，導致無法使用，限期3天支付贖金，不付錢則毀損解密金鑰，檔案永遠救不回來。
勒索軟體的主要影響
無法使用作業系統(限制作業系統存取)無法開啟某些檔案(檔案加密)開機時出現勒索畫面
5


Ooops, your files have been encrypted!
Chinese (traditiona
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪
Payment will be raised on
1/4/1970 08:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 08:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

被勒索當下即時處置

- 斷開網路連線
- 馬上關機 (10分鐘內還有殘存資料可以救回..看電腦速度)
- 保留電腦 通報資訊人員
- 不要付錢


單靠過往的漏洞修補是無法面對新型攻擊的，
畢竟漏洞是找不完的!
未來企業面對資安風險，更應強調
“感知能力”與“遭受攻擊時的快速應對”

後續處置事項

- 暫時停止該員電腦網路存取登入權限
- 檢查權限可以寫入公用資料夾是否感染
- 資料備份還原 /外接HD救資料
- 查找出勒索程式來源
- T-clean 掃描後送Trend Micro分析
- 安裝啟用防毒軟體防勒索行為控管

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

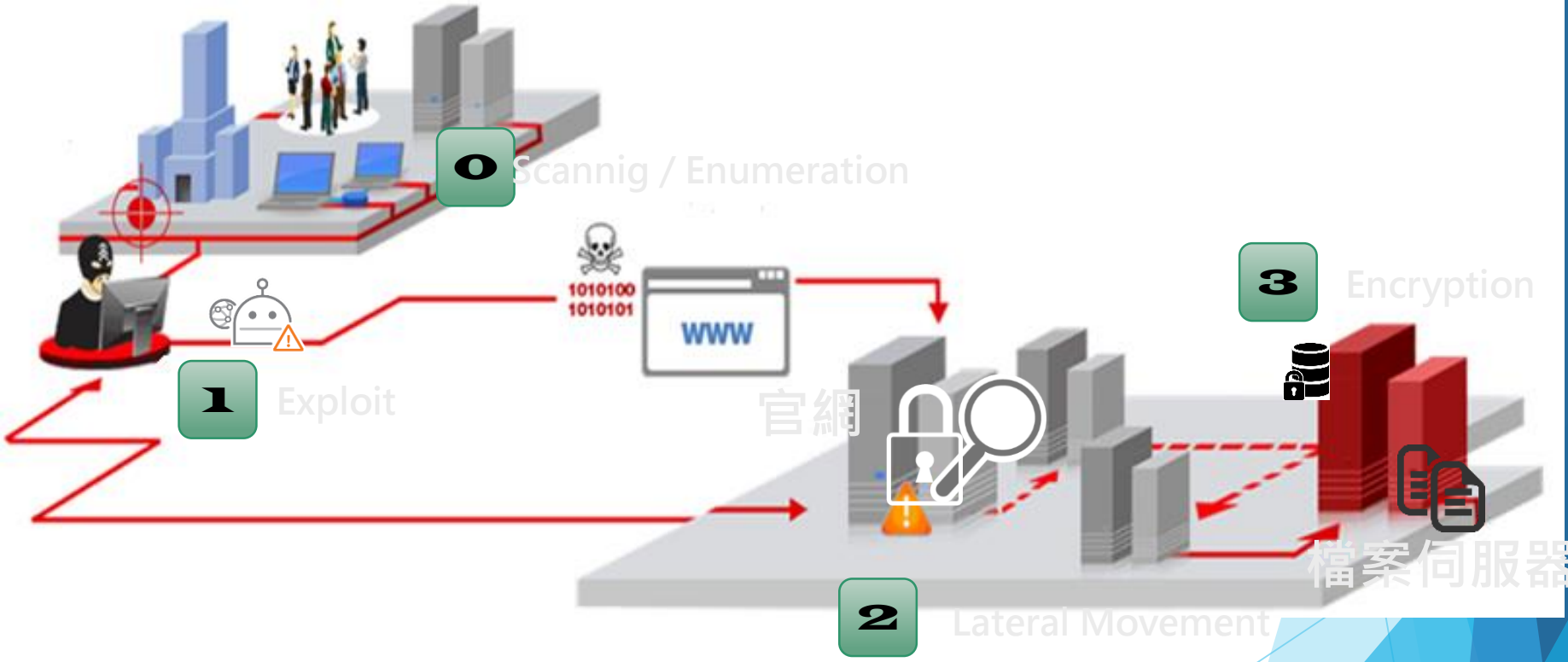
階段	事前預防	即時處置	事後宣導
作法	●定期更新軟體	●斷網關機	●事件分析
	●只打開信任的郵件	●清查受損範圍	●人員教育
	●安全防護軟體	●資料復原	●權限管控
	●定期備份檔案		●強化防護

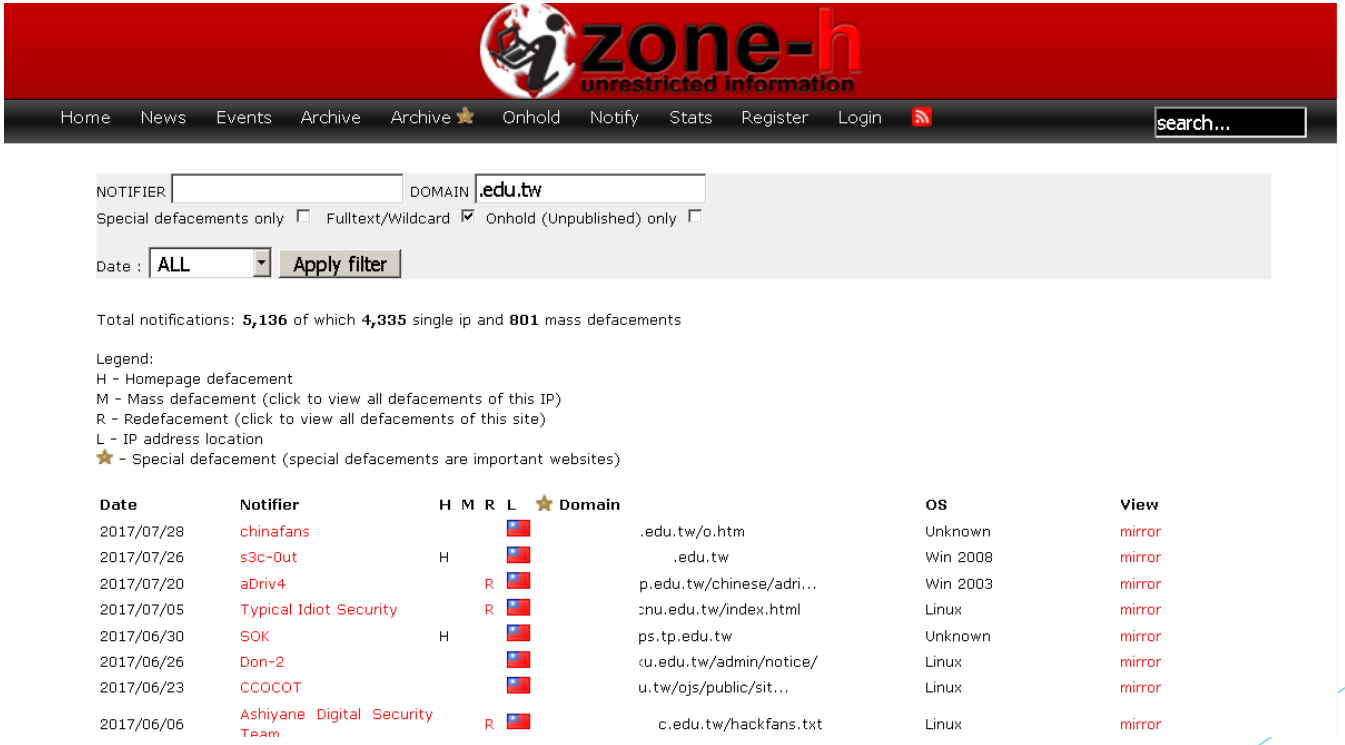
資料來源：趨勢提供，iThome 整理，2016 年 7 月

Agenda

- 引言
- 資安威脅趨勢
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

勒索軟體攻擊新型態


0
Scannig / Enumeration
1010100
1010101
WWW
1
Exploit
官網
3
Encryption
檔案伺服器
2
Lateral Movement


zone-h
unrestricted information
Home News Events Archive Archive Onhold Notify Stats Register Login
search...
NOTIFIER DOMAIN .edu.tw
Special defacements only Fulltext/Wildcard Onhold (Unpublished) only
Date : ALL Apply filter
Total notifications: 5,136 of which 4,335 single ip and 801 mass defacements
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
- Special defacement (special defacements are important websites)
Date Notifier H M R L Domain OS View
2017/07/28 chinafans .edu.tw/o.htm Unknown mirror
2017/07/26 s3c-0ut H .edu.tw Win 2008 mirror
2017/07/20 aDriv4 R p.edu.tw/chinese/adri... Win 2003 mirror
2017/07/05 Typical Idiot Security R cnu.edu.tw/index.html Linux mirror
2017/06/30 SOK H ps.tp.edu.tw Unknown mirror
2017/06/26 Don-2 u.edu.tw/admin/notice/ Linux mirror
2017/06/23 CCOCOT u.tw/ojs/public/sit... Linux mirror
2017/06/06 Ashiyane Digital Security Team R c.edu.tw/hackfans.txt Linux mirror

免費的WIFI...最貴...

- 若您非得連上開放的熱點不可，請切記只用它來連上一些新聞網站、觀賞 YouTube 影片，或是爆笑圖片分享之類的網站。切勿透過開放的 Wi-Fi 網路連上一些您不希望陌生人在旁邊偷窺的網站或是您的網路帳號

隨插隨充...真的安全嗎

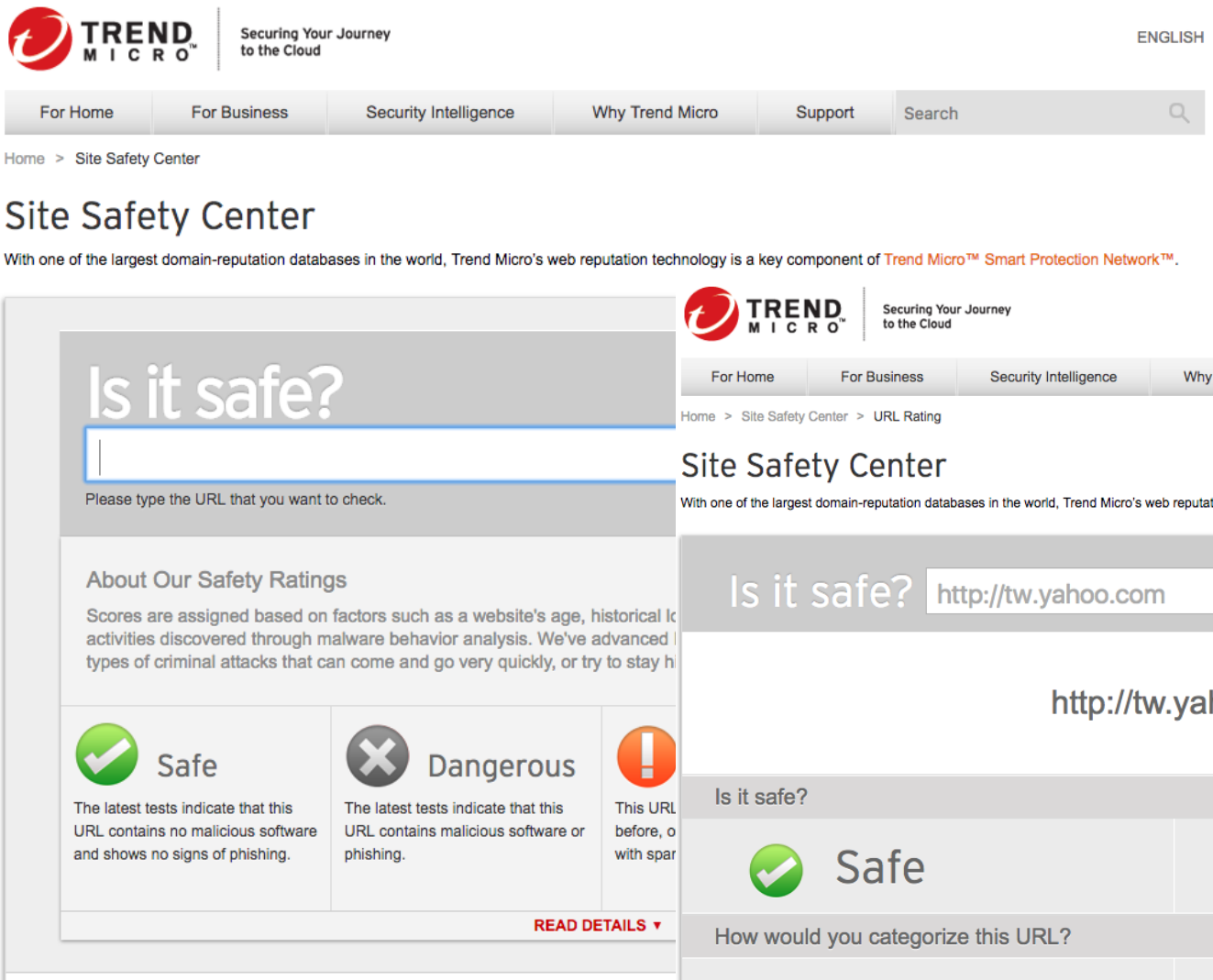

安全 https://www.165.gov.tw/loss_rank.aspx
165全民防騙超連結
內政部警政署
NATIONAL POLICE AGENCY
165反詐騙諮詢專線
165 首頁
新聞資訊
成立宗旨
組織編制
搜尋
這個頁面上的內容需要較新版本的 Adobe Flash Player。
Get ADOBE FLASH PLAYER
我要檢舉
我要報案
案件查詢
詐騙闢謠專區
詐騙小叮嚀
高詐欺風險賣場排名
竄改來電號碼排名
詐欺預防寶典
詐欺刑責
影音下載
海報宣導
新聞快訊
詐騙闢謠專區
詐騙小叮嚀
民眾通報高風險
竄改來電號碼排
民眾通報高風險賣場排名
排名
內容
更新日期
1 饗食天堂 件數：39件 2017/6/21
2 奇摩拍賣 件數：38件 2017/6/21
3 EZ訂（電影票券） 件數：27件 2017/6/21
4 雄獅旅行社 件數：21件 2017/6/21
5 旋轉拍賣、露天拍賣 件數：14件 2017/6/21
6 ViVa美好購物網 件數：10件 2017/6/21
7 統計日期：106年6月12日至106年6月18日 2017/6/21

你還在用相同帳密四處走嗎?

Agenda

- 引言
- 資安威脅趨勢
- 網路勒索之年
- 案例分享
- 如何因應與面對
- Q&A

相信安全？


TREND MICRO
Securing Your Journey to the Cloud
ENGLISH
For Home
For Business
Security Intelligence
Why Trend Micro
Support
Search
Home > Site Safety Center
Site Safety Center
With one of the largest domain-reputation databases in the world, Trend Micro's web reputation technology is a key component of Trend Micro™ Smart Protection Network™.
Is it safe?
Please type the URL that you want to check.
About Our Safety Ratings
Scores are assigned based on factors such as a website's age, historical lo
activities discovered through malware behavior analysis. We've advanced
types of criminal attacks that can come and go very quickly, or try to stay hi
Safe
The latest tests indicate that this URL contains no malicious software and shows no signs of phishing.
Dangerous
The latest tests indicate that this URL contains malicious software or phishing.
This URL
before, o
with spar
READ DETAILS
TREND MICRO
Securing Your Journey to the Cloud
ENGLISH
For Home
For Business
Security Intelligence
Why Trend Micro
Support
Search
Home > Site Safety Center > URL Rating
Site Safety Center
With one of the largest domain-reputation databases in the world, Trend Micro's web reputation technology is a key component of Trend Micro™ Smart Protection Network™.
Is it safe?
http://tw.yahoo.com
CHECK NOW
http://tw.yahoo.com
Is it safe?
Safe
The latest tests indicate that this URL contains no malicious software and shows no signs of phishing.
How would you categorize this URL?
Search Engines / Portals
Search engine sites or portals that provide directories, indexes, or other retrieval systems for the Web

如何面對不可預期的威脅?

- 預防重於治療?
- 災難永遠發生在不可預期處
- 以實體世界災難為例:
  - 安全觀念的建立
  - 落實的安全檢查
  - 即時的監測與通報機制
  - 事件發生後的緊急應變流程
  - 確實的事件原因調查與分析
  - 重新檢討上述流程的缺失
  - 改善現有流程或建立新流程

別讓資安事件成為貴單位的”八仙塵爆”

還有...

- 依照案例分析攻擊手法，都是社交工程方式，建議加強社交工程警覺訓練,尤其是網站及郵件的相關警覺及認知
- 重新檢視共享資料夾的權限開放，例如:不要開放Everyone Full Control權限。
- 建議檢視網域帳號安全，避免網域使用公用帳號。
- 定期修補作業系統與應用程式的漏洞。
  - Java
  - Flash
  - IE
  - …

趨勢科技免費釋出勒索軟體解

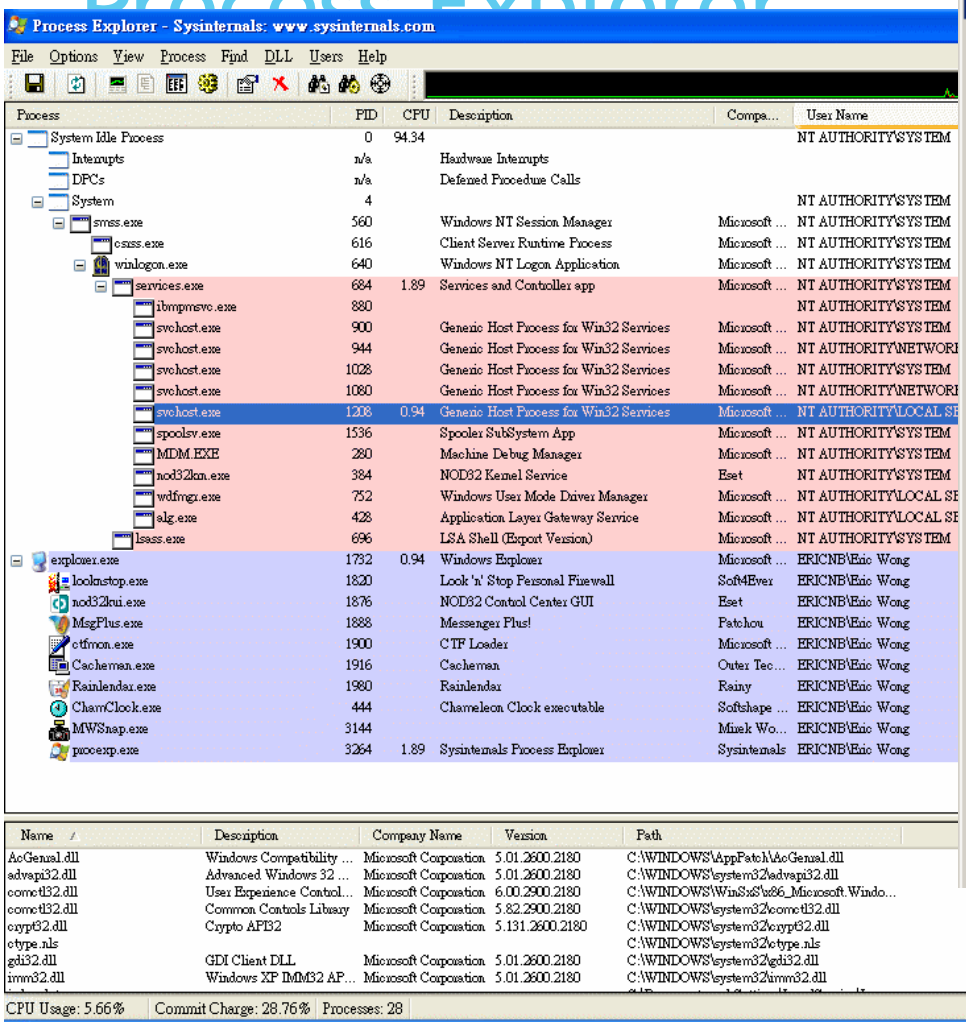
主要是針對Cryptxxx 2.0版和TeslaCrypt v1、v3和v4版勒索軟體加密的檔案

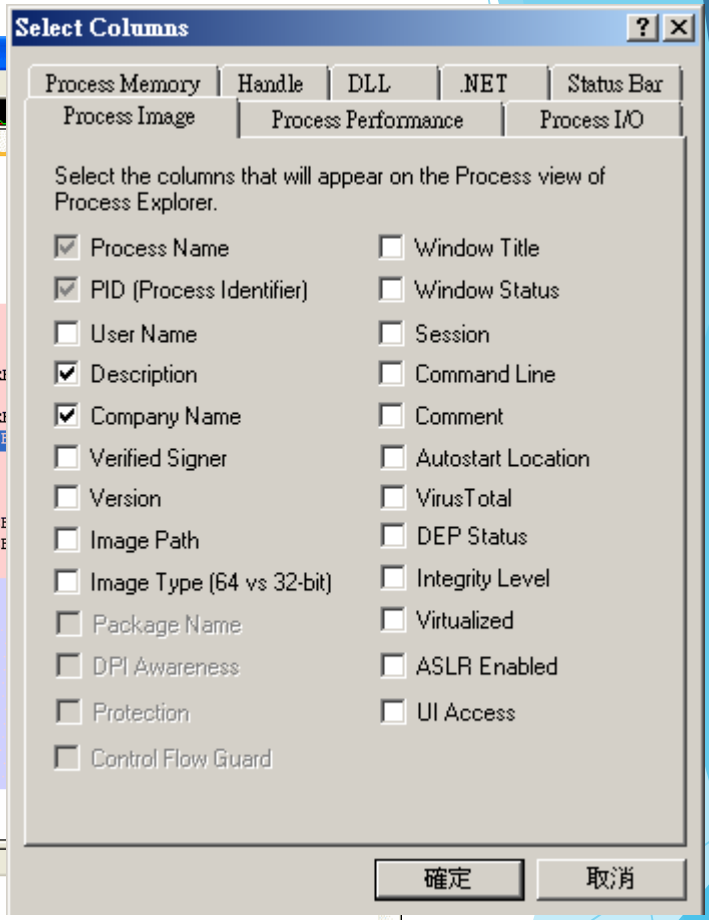
http://esupport.trendmicro.com/media/13656199/RansomwareFileDecryptor%201.0.1523%20MUI.zi

採購家用智慧型裝置時應注意的安全考量

- 智慧型裝置是否具備安全認證功能？
- 智慧型裝置在首次安裝時是否會要求您變更使用者名稱和密碼?
- 我的密碼強度如何？
- 智慧型裝置更新方便性如何？
- 智慧型裝置是否會將韌體更新和網路通訊確實加密？
- 智慧型裝置是否需要開放任何連接埠？
- 智慧型裝置如何處理電量不足或電池耗盡的問題？
- 製造商面對裝置漏洞的處理能力如何？

Process Explorer

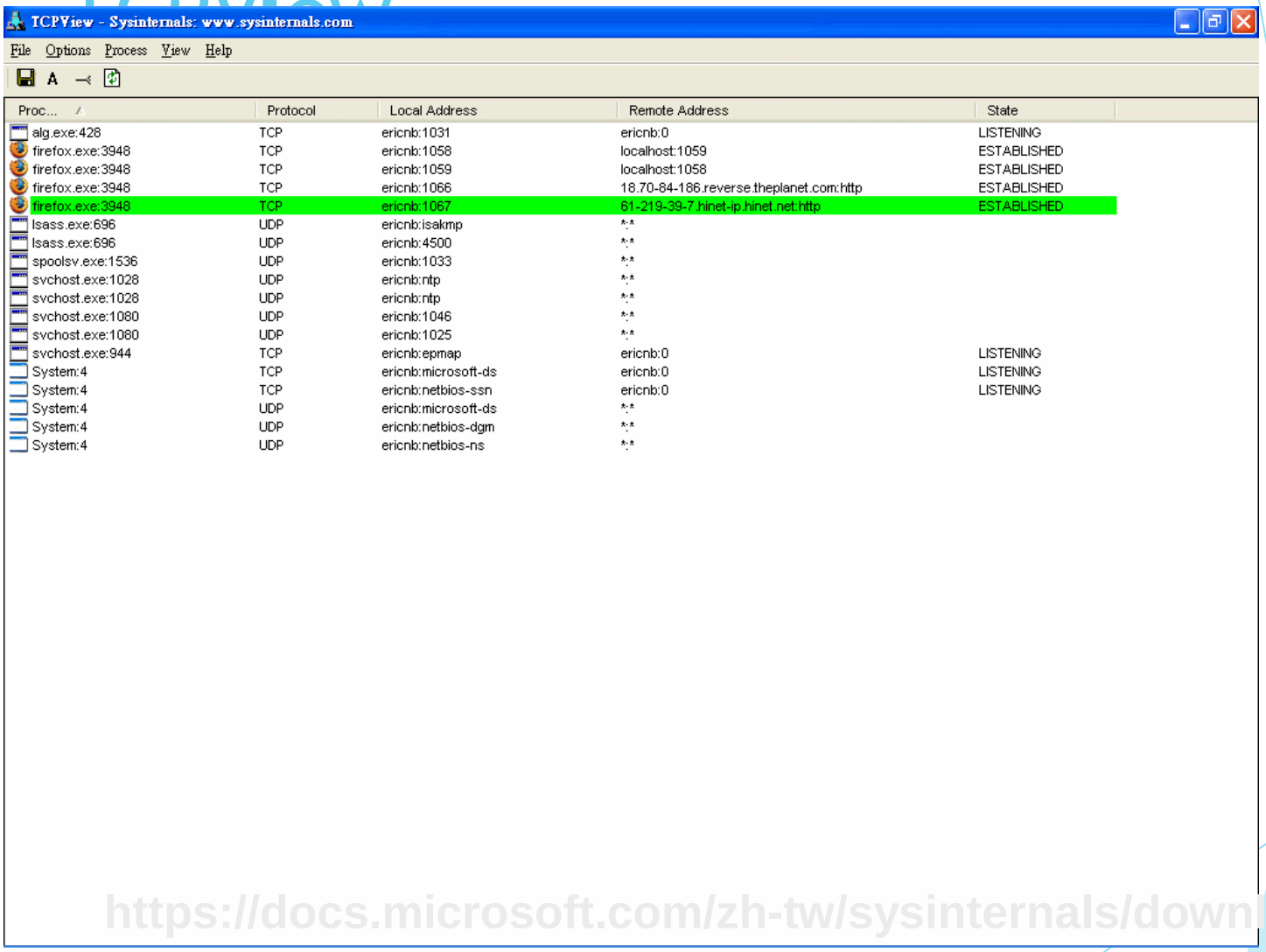




同檔名、不同存放目錄

https://docs.microsoft.com/zh-tw/sysinternals/downloads/process-explorer

TCPView



https://docs.microsoft.com/zh-tw/sysinternals/downloads/tcpview

VirusTotal 是一項免費服務，可**分析可疑檔案和網址**，並有助於快速偵測病毒、蠕蟲、特洛伊木馬和所有種類的惡意軟體。

檔案 URL 搜尋

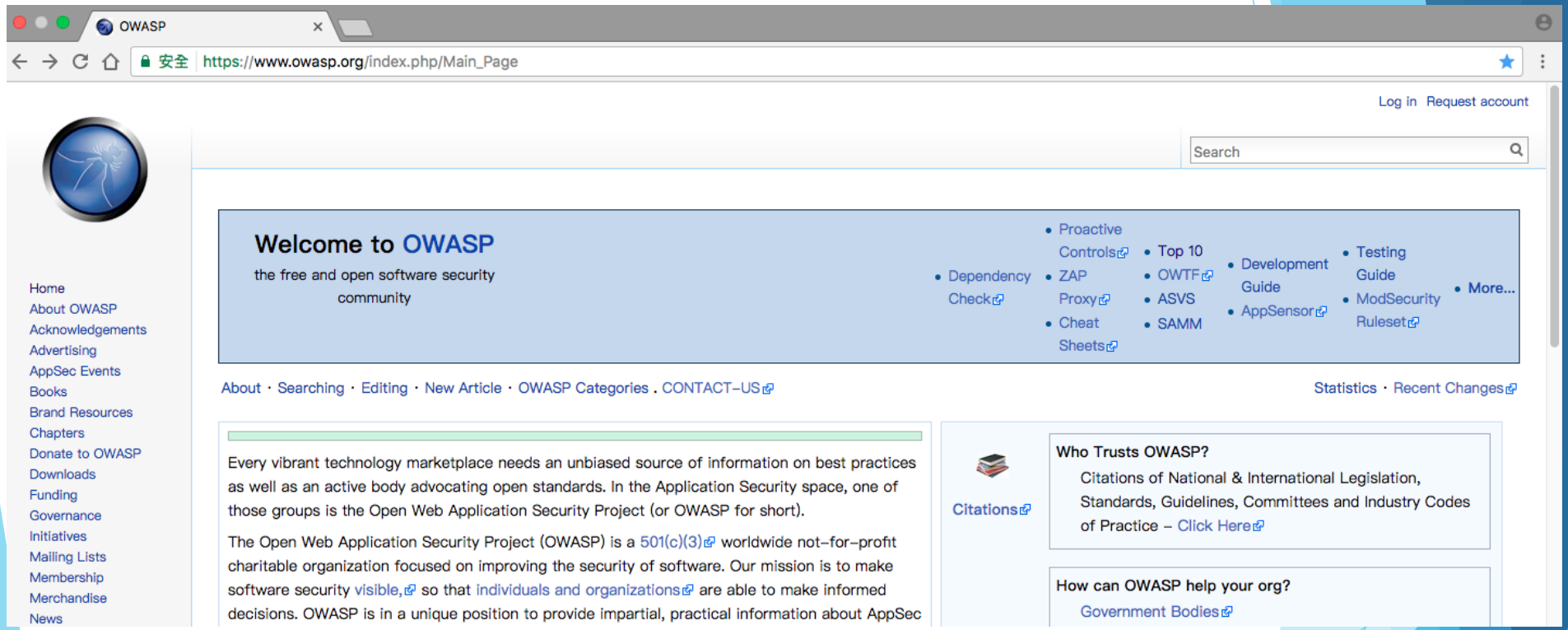
未選擇檔案 選擇檔案

最大檔案大小: 128MB

按下【掃瞄!】，即表示您同意我們的 服務條款 並允許 VirusTotal 將此檔案與安全社群共用。 請參閱我們的 隱私權原則 了解詳情。

掃瞄!

https://www.virustotal.com/zh-tw/


OWASP
安全 https://www.owasp.org/index.php/Main_Page
Log in Request account
Search
Welcome to OWASP
the free and open software security community
Dependency Check
Proactive Controls
ZAP Proxy
Cheat Sheets
Top 10
OWTF
ASVS
SAMM
Development Guide
AppSensor
Testing Guide
ModSecurity Ruleset
More...
Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
News
About · Searching · Editing · New Article · OWASP Categories . CONTACT-US
Statistics · Recent Changes
Every vibrant technology marketplace needs an unbiased source of information on best practices as well as an active body advocating open standards. In the Application Security space, one of those groups is the Open Web Application Security Project (or OWASP for short).
The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec
Citations
Who Trusts OWASP?
Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice – Click Here
How can OWASP help your org?
Government Bodies


資安趨勢觀測站
soc.nchc.org.tw/news/news_list.php
資安趨勢觀測站
Facts on Internet Risks and Security Threats
資安快訊
弱點與漏洞資訊
資安統計數據
惡意程式分析服務
弱點掃描服務
網路資安資源
關於我們
Facts on Internet Risks and Security Threats
最新消息
發佈日期
消息摘要
2017-07-26
微軟雲端版AI抓蟲工具Security Risk Detection出爐，協助開發者抓漏
2017-07-26
又一加密貨幣服務商Veritaseum被駭，損失840萬美元
2017-07-26
全球駭客高手齊聚拉斯維加斯，讓飯店業很駭怕
2017-07-21
防國家級監控？ Tor也推抓漏獎勵計畫
2017-07-21
鎖定「SambaCry」漏洞的新威脅現身， Linux 使用者請盡速更新系統
2017-07-20
災難！CoinDash首度發行貨幣當天就被駭，損失近700萬美元
資安燈號
依照我們專業的判斷，目前整體資安狀態，我們出現如下燈號。
數據綜圖
我們精心計算90天攻擊IP總數
相關連結
NARLabs 國家實驗研究院

Windows 設定篇

定期更新作業系統的Hotfix

- 「我的電腦」右鍵 >>「內容」>>「自動更新」>> 自動(建議選項) >> 選取更新及安裝的時間

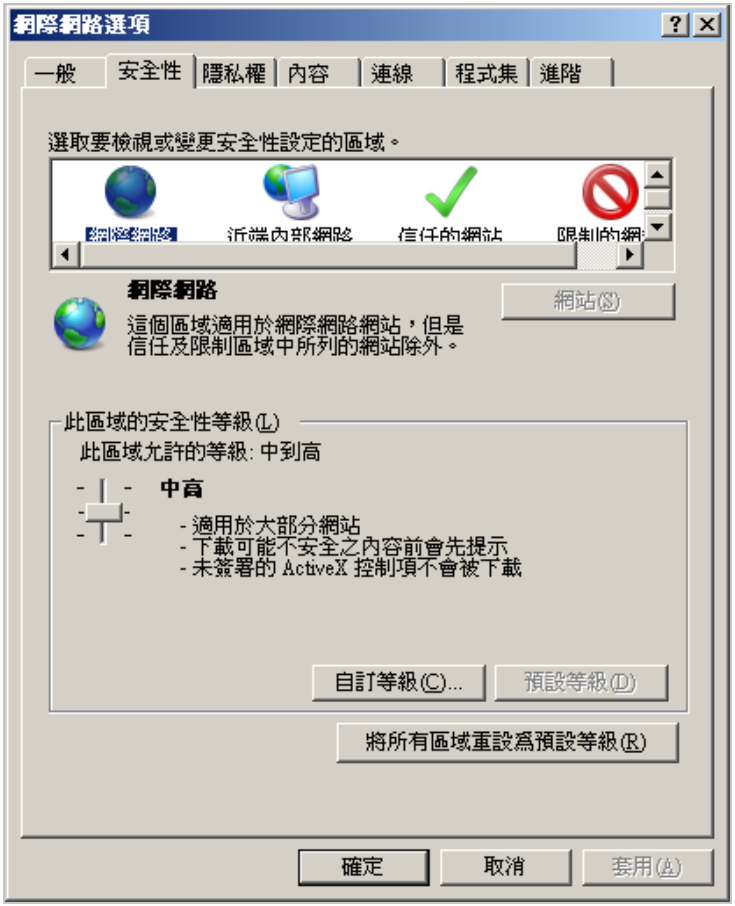
Windows 設定篇

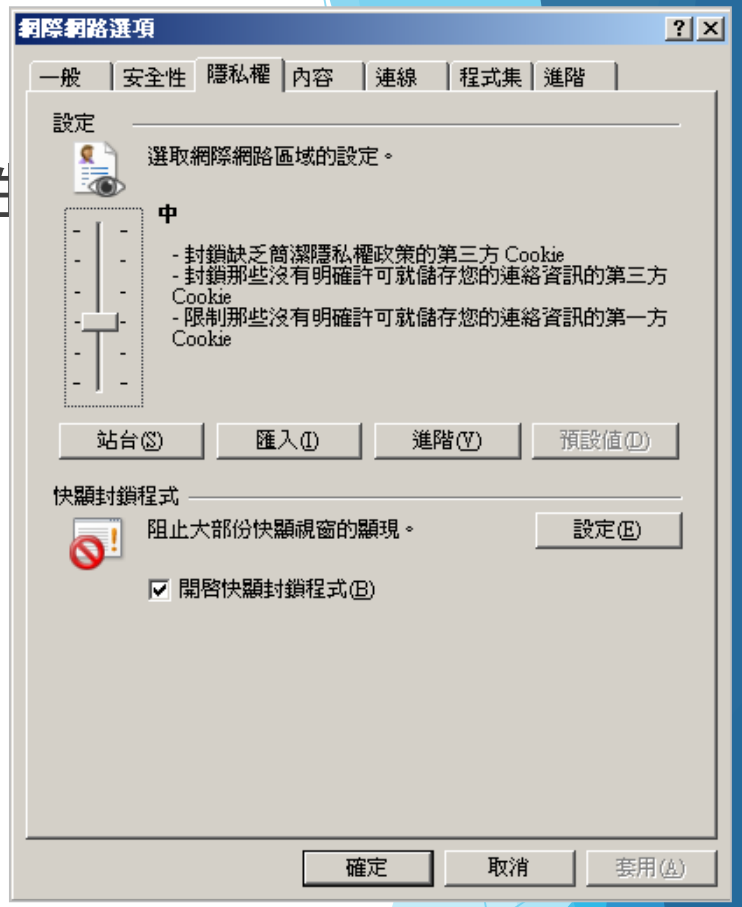
開啟IE的網路釣魚篩選工具

- 開啟IE
- 工具 >> 網路釣魚篩選工具 >> 開啟自動網站檢查

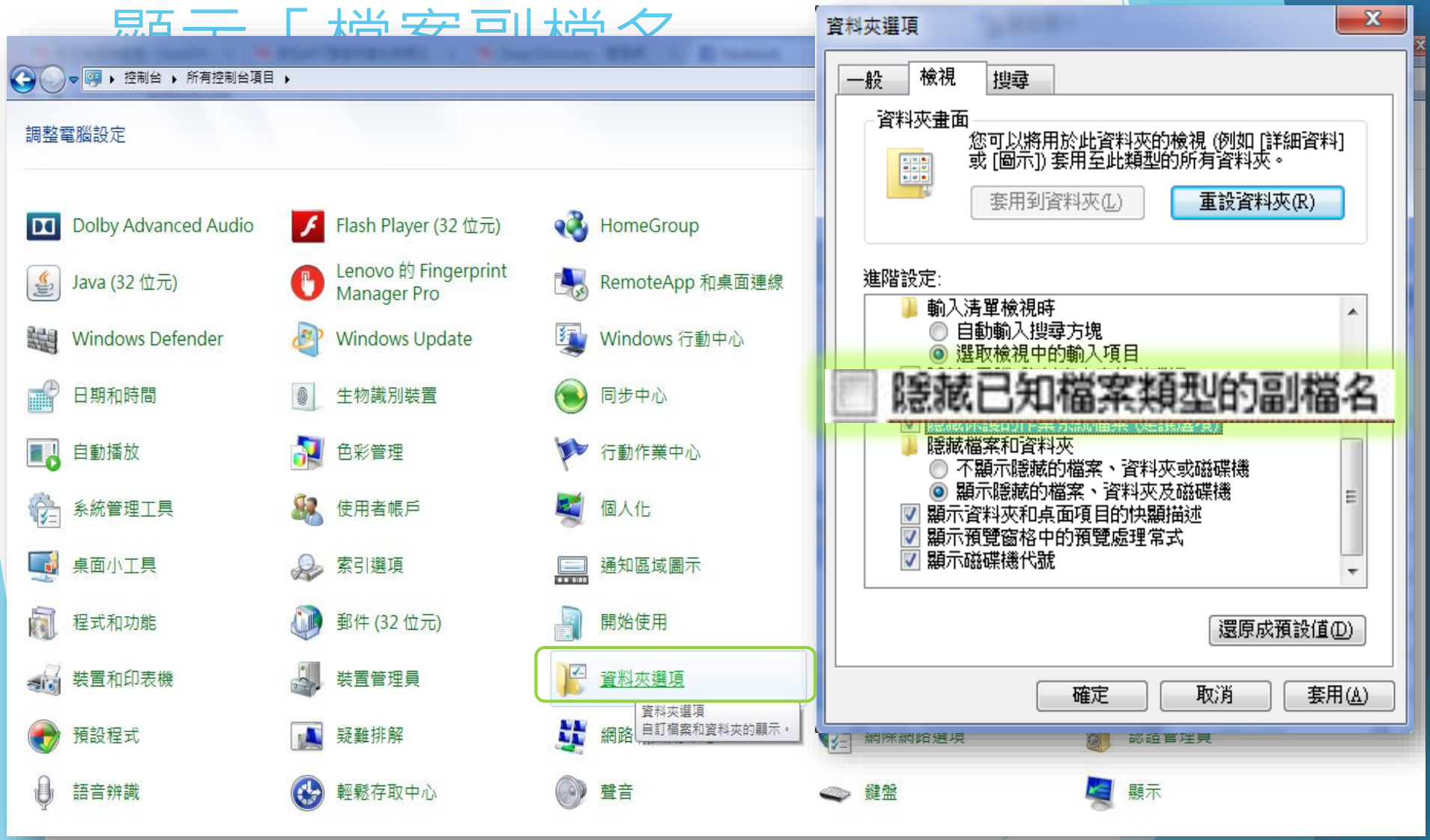
Windows 設定篇

- 設定IE安全層級設定至少是 [中安全性
- 開啟快顯封鎖程式

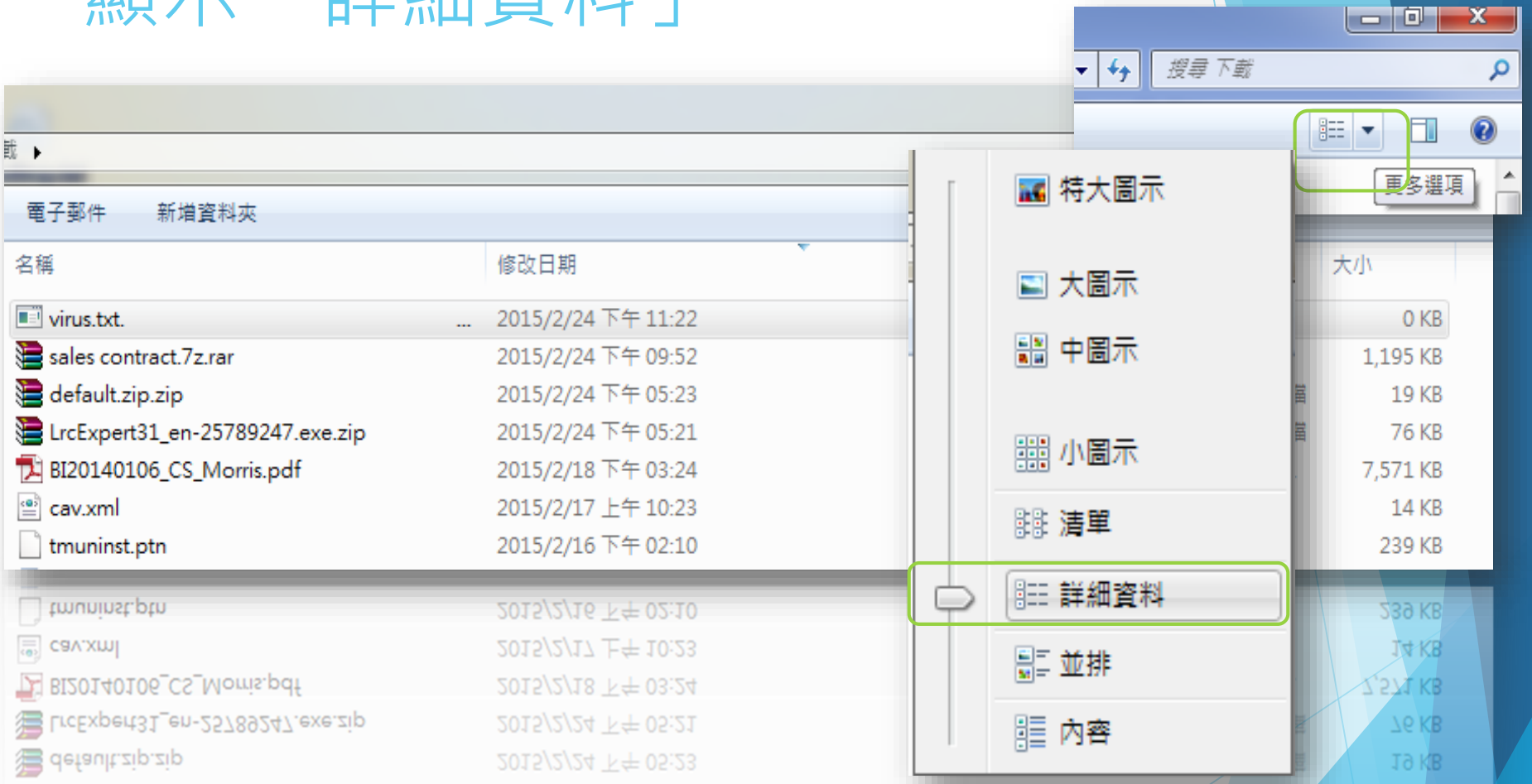




顯示「檔案副檔名


控制台 ▸ 所有控制台項目 ▸
調整電腦設定
Dolby Advanced Audio
Flash Player (32 位元)
HomeGroup
Java (32 位元)
Lenovo 的 Fingerprint Manager Pro
RemoteApp 和桌面連線
Windows Defender
Windows Update
Windows 行動中心
日期和時間
生物識別裝置
同步中心
自動播放
色彩管理
行動作業中心
系統管理工具
使用者帳戶
個人化
桌面小工具
索引選項
通知區域圖示
程式和功能
郵件 (32 位元)
開始使用
裝置和印表機
裝置管理員
資料夾選項
預設程式
疑難排解
網路
語音辨識
輕鬆存取中心
聲音
資料夾選項
自訂檔案和資料夾的顯示。
資料夾選項
一般
檢視
搜尋
資料夾畫面
您可以將用於此資料夾的檢視 (例如 [詳細資料] 或 [圖示]) 套用至此類型的所有資料夾。
套用到資料夾(L)
重設資料夾(R)
進階設定:
輸入清單檢視時
自動輸入搜尋方塊
選取檢視中的輸入項目
隱藏已知檔案類型的副檔名
隱藏檔案和資料夾
不顯示隱藏的檔案、資料夾或磁碟機
顯示隱藏的檔案、資料夾及磁碟機
顯示資料夾和桌面項目的快顯描述
顯示預覽窗格中的預覽處理常式
顯示磁碟機代號
還原成預設值(D)
確定
取消
套用(A)
鍵盤
顯示

顯示「詳細資料」


搜尋 下載
更多選項
電子郵件
新增資料夾
名稱
修改日期
大小
virus.txt.
2015/2/24 下午 11:22
0 KB
sales contract.7z.rar
2015/2/24 下午 09:52
1,195 KB
default.zip.zip
2015/2/24 下午 05:23
19 KB
LrcExpert31_en-25789247.exe.zip
2015/2/24 下午 05:21
76 KB
BI20140106_CS_Morris.pdf
2015/2/18 下午 03:24
7,571 KB
cav.xml
2015/2/17 上午 10:23
14 KB
tmuninst.ptn
2015/2/16 下午 02:10
239 KB
特大圖示
大圖示
中圖示
小圖示
清單
詳細資料
並排
內容

防範社交工程郵件重點

- 不是所屬業務信件一律不開
- 陌生郵件一律不開!!!
- 不要太八卦, 怪怪的郵件不要再轉寄!!
- 注意連結與附檔
  - Com
  - Exe
  - Scr
  - Lnk
  - Bat

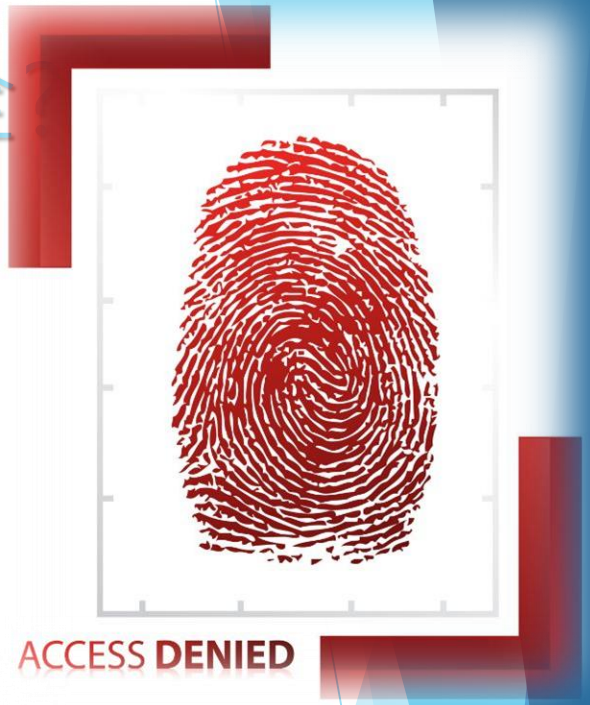
勒索病毒曾經使用過的網路釣魚主旨或手法包含:

- 退稅通知
- 電子帳單/電子發票
- Google Chrome 和 Facebook 重大更新和通知訊息
- 假冒com 訂單出貨通知
- iPhone中獎通知
- 求職信/履歷表
- 電子訃聞
- 誘騙使用者連到看似真正銀行或政府機構網站的假網頁
- 輸入驗證碼（CAPTCHA，一種防止機器人的程序）
- 您的帳戶欠款已過期!

可疑檔案掃瞄網站 https://www.virustotal.com/en-gb/

可疑網址檢查網站 http://global.sitesafety.trendmicro.com/

如何在上網瀏覽時保持安全



- 採用具備安全防護功能的應用程式
- 持續定期更新
- 按下連結時應提高警覺
- 禁止非必要的通訊協定進入企業網路
- 定期更新作業系統
- 建置多面向的多層式安全防護解決方案
- Web Threat Protect (WTP)避免電腦被傀儡網路控制

趨勢科技免費工具 – 網頁威脅防禦

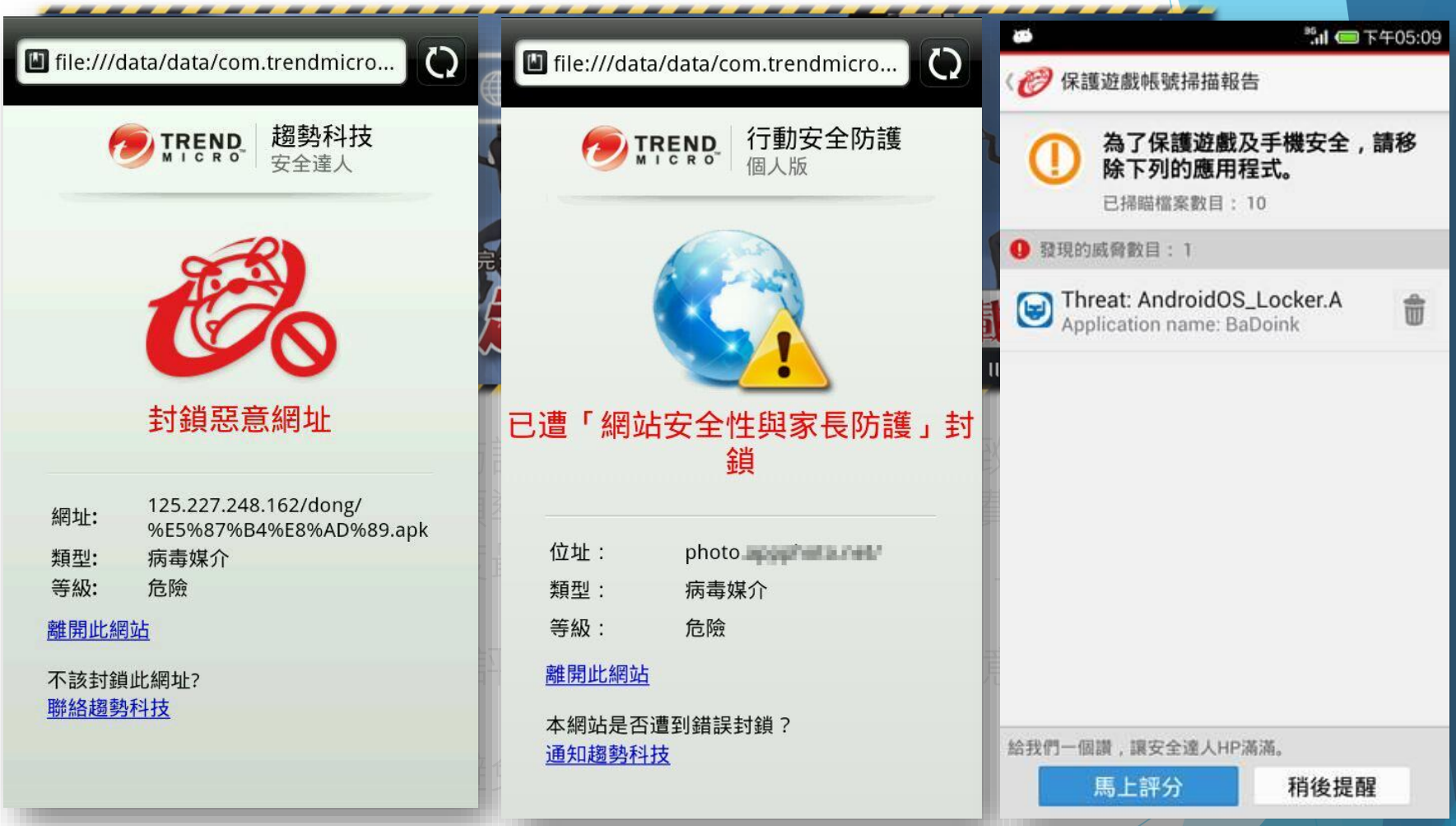
WTP 網頁威脅防禦工具

- 猶如線上大型掃毒引擎，為你偵測並阻擋變種新病毒
- 有效防止Downloader病毒下載器，在背景偷偷自動下載病毒
- 能與您電腦上既有的防毒軟體同時安裝、相互支援，完整彌補重要的安全漏洞
- 避免讓你瀏覽或連結至惡意網站，降低與被植入惡意程式或掛馬網頁接觸的機會
- 當偵測到網頁威脅或Bot 程式等相關可疑行為，會立即跳出警訊通知

http://www.trendmicro.com.tw/wtp/micro/index.asp


已由趨勢科技封鎖 - Windows Internet Explorer
http://wrs50.winshipway.com/
Bing
我的最愛
建議的網站
網頁快訊圖庫
已由趨勢科技封鎖
網頁(P)
安全性(S)
工具(O)
已由趨勢科技封鎖
Trend Micro WTP Add-On 已經將此網頁識別為不適當的網頁。
位址：
http://wrs50.winshipway.com/
WTP Add-On 不應該封鎖此網頁，請按一下此按鈕通知趨勢科
cro Incorporated/趨勢科技股份有限公司。保留所有權利。
網際網路 | 受保護模式: 關閉
Trend Micro WTP A...
下午 02:44
Trend Micro WTP Add-On
TREND MICRO WTP Add-On
Trend Micro Web Protection Add-On (WTP Add-On) - 網友十大必備免費上網防護工具！有效且主動防護您的電腦免受網頁威脅或遭到僵屍病毒的攻擊，並能偵測秘密控制您的電腦以從事網路犯罪的可疑行為。
已成功阻擋惡意網頁！
已檢查 34 個網址，並成功封鎖 2 個試圖感染的威脅。
清除記錄
全球網頁威脅資訊
記錄
設定
Trend Micro™ WTP Add-On
已成功阻擋網頁威脅！
WTP Add-On已成功阻擋惡意網頁攻擊您的電腦。您可按一下「最佳上網防護」取得更完整的上網安全防護軟體，以徹底清除電腦中的安全威脅。
最佳上網防護

安全達人(完全免費，提供宅急便詐騙簡訊防護、手機防毒)



http://tmms.cloudsupport.trendmicro.com/download/gmobi?channel=TM.com

~ Thank You ~