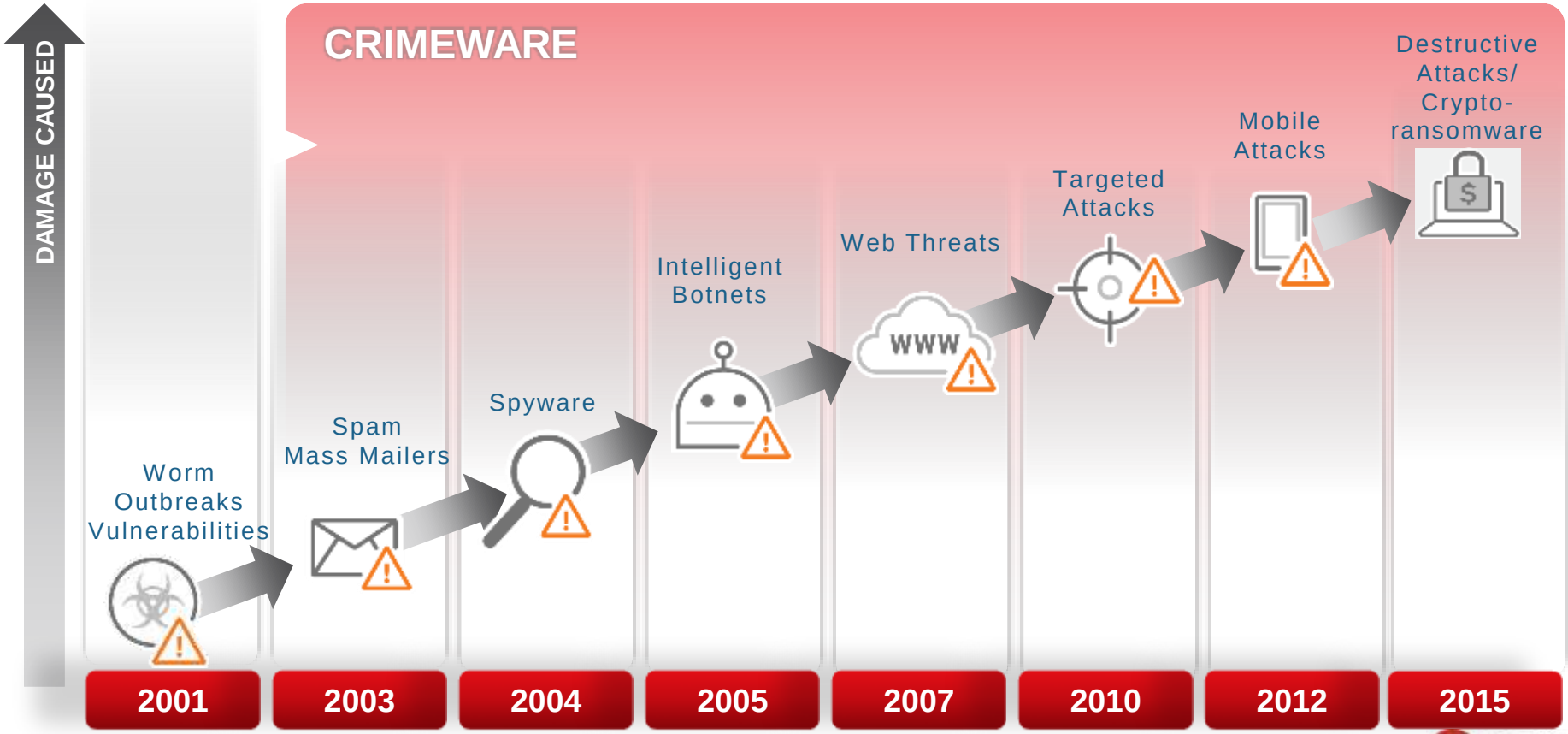
家庭電腦網絡面對之威脅及防護

黃嘉敏 Carmen Wong
趨勢科技 Security Consultant

Facebook「XXX Video」

- 2016年9月12日
- Facebook account 遭到惡意程式的竊取

威脅演變

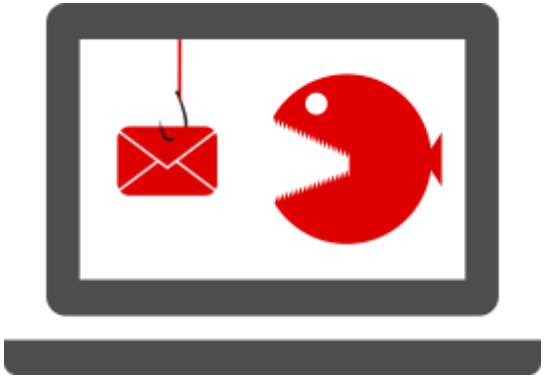


Agenda

- 電子郵件詐騙
  - 網絡釣魚 (Phishing)
  - 商務電子郵件入侵 (BEC)
- 勒索程式
- IOE萬物聯網

網絡釣魚

- 用電話、電郵、即時通訊或傳真獲取用戶個人資料以竊取用戶身分的一種手法。
- 多數網絡釣魚看似具備合法用途，但實際上是設計用來從事不法活動。



網路釣魚

一個簡單的測試

（1）http://w www.google.com

（2）http://w www.yahoo.com

（3）（按這裡 www.yahoo.com

（4） www.yahoo.com

From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

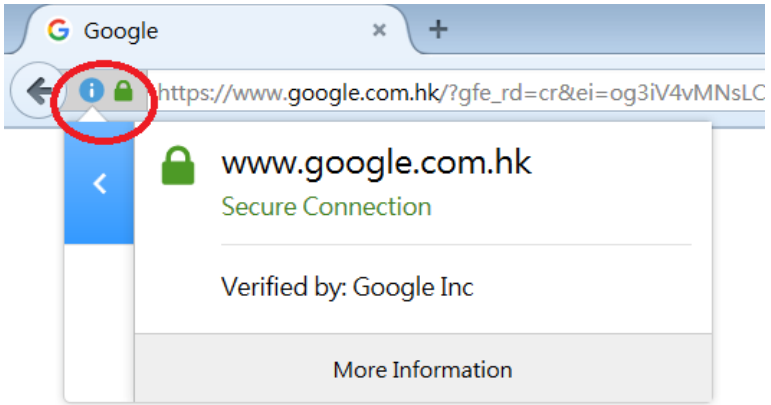
TREND MICRO

網路釣魚

- 為什麼要盜用這些個資?對我有傷害嗎?
  - 販賣個資
  - 發動下一波的攻擊

電郵保安

- 不要隨意開啟來歷不明的電郵
- 在開啟電郵附加檔之前先進行掃描
- 檢查郵件內是否有拼寫錯誤 - 寄信人
- 點選連結前,先移動滑鼠檢查真實來源
  - b和d， O和0，l和1
- 常用網站加入書籤
- 證書認証



TREND MICRO

「商務電子郵件入侵」(Business Email Compromise，簡稱 BEC)

- 中間人電子

最常成為 BEC 詐騙電子郵件目標的公司人員

第三種版本：入侵電

最常收到假冒企業高層的變臉詐騙郵件對象為CFO(40.38%)

TREND MICRO

Tips

- 小心處理來自高階主管的不尋常郵件(針對要求資金轉移)。
- 廠商變更的匯款資訊，須由公司另一位人員複核。
- 掌握合作廠商的習慣：匯款的詳細資料和原因。
- 使用電話做為雙重認證機制 (撥打登記的慣用電話號碼)
- 提升員工防詐意識：積極做好員工訓練，培養良好的資安習慣。
- 一旦遇到任何詐騙事件，立即報警。

勒索程式

勒索軟體：不給錢，把你電腦變磚塊！

定義、原理和後果

什麼是勒索程式？

勒索程式是一種會挾持資料的嚴重資安威脅，它會讓檔案和系統功能無法使用，甚至讓整台電腦都無法使用。受害者必須支付一筆贖金來贖回自己的檔案和系統。

TREND MICRO

勒索軟體特質

1. **把你的檔案當作人質**
   - 加密重要文件
2. **無法自行解密**
   - 使用 AES 和 RSA 演算法
3. **清除病毒將無法復原**
   - 毒沒了，但檔案還沒解密
4. **向駭客購買解密鑰匙**
   - 使用Bitcoin交易
   - 通常能復原，維持口碑

勒索程式

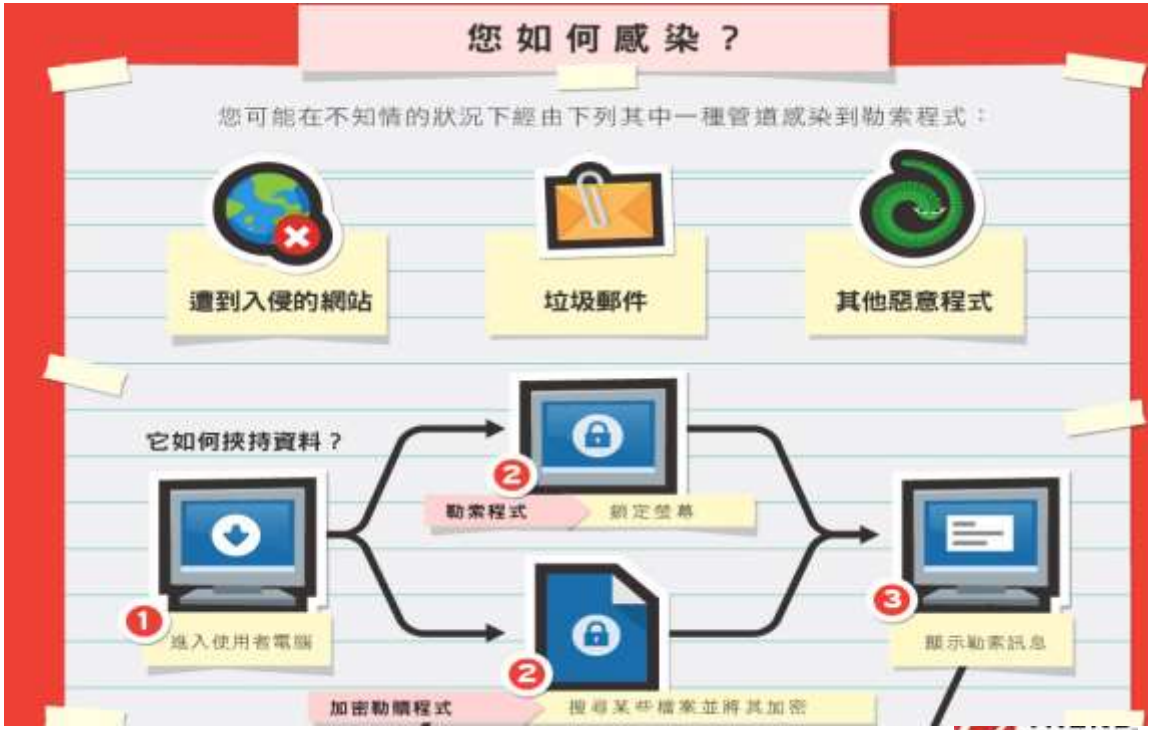
2016年首8個月
263宗,較去年上升4.5倍
首半年全球損失超過2億美元

Source: TrendLabs 2016 1H Report

勒索軟體的散播途徑

- 目前主要的攻擊途徑

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



打開 Word 檔也會中勒索軟體

- Locky透過電子郵件進入受害者電腦，偽裝成發票並附上帶有惡意巨集的Word文件

TREND MICRO

入侵靠漏洞

- 0-Day 漏洞
- 已知漏洞

CVE ID	Application	Issue Date	Exploit Kit	Publish Date of Exploit Kit Support	Time Difference
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

01 使用者未更新程式

e.g. 使用舊版Flash Player

02 利用Flash的漏洞

使用者瀏覽正常網頁，

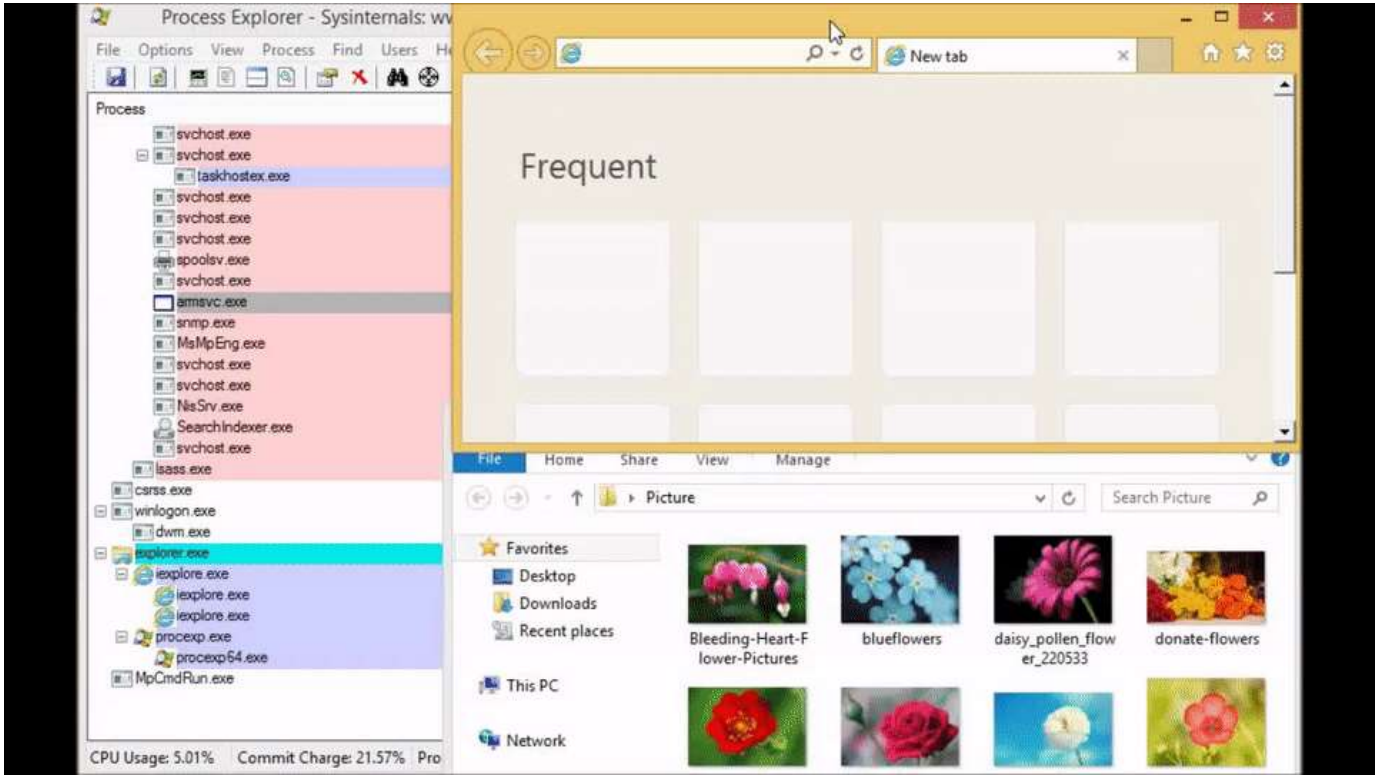
04 Downloader被執行後，便會下載完整的勒索軟體並執行。

勒索軟體一旦執行，使用者的檔案就會被加密。

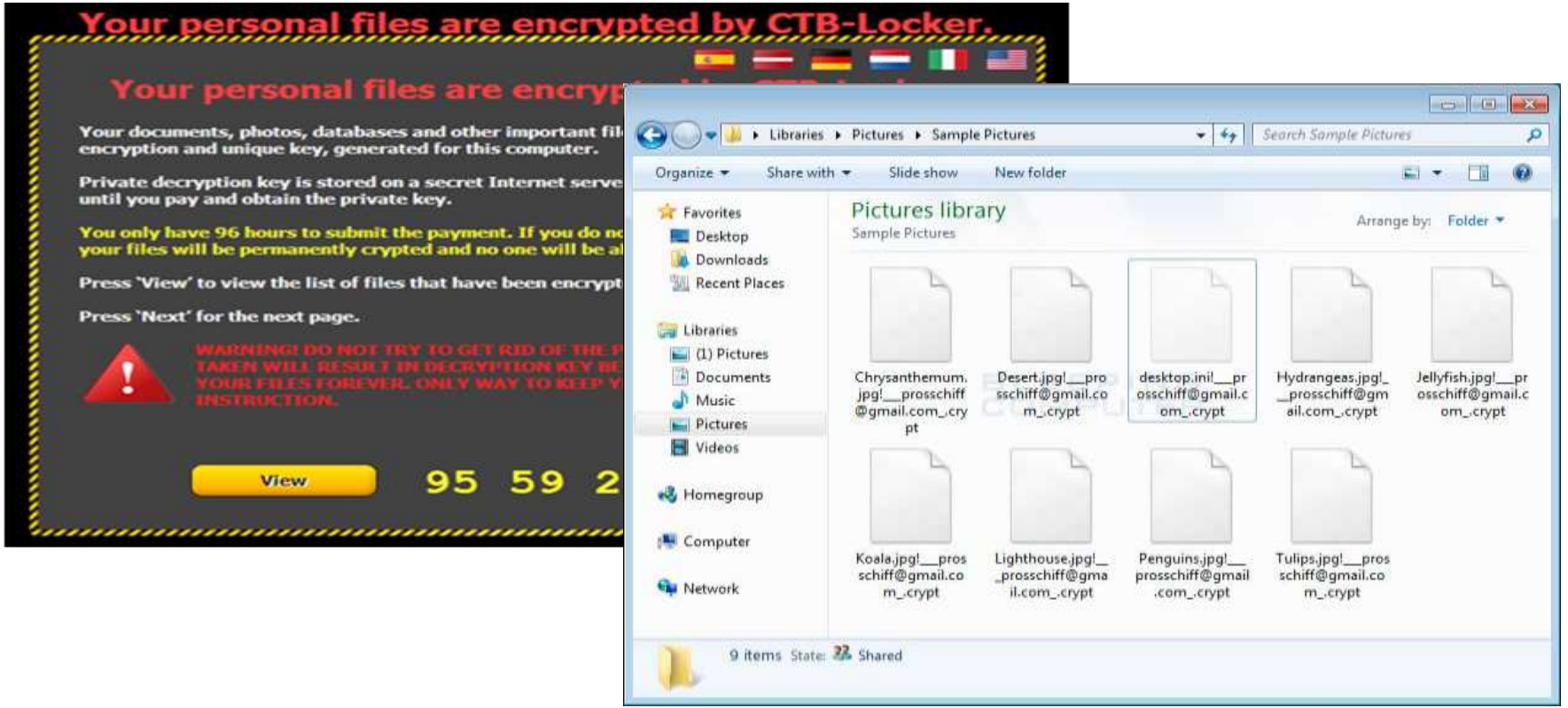
下載勒索軟體　執行勒索軟體　檔案加密

TREND MICRO 趨勢科技

當進入了被掛馬的網站



勒索畫面



Chimera 勒索軟體:要被駭還是一起駭人賺黑心錢？

- 除了勒索之外…
- 邀請受害者當合作夥伴??

Not Only Computer

Android

NAS - Synology

預防勒索軟體綁架電腦 三不三要

不上鉤:
標題特別吸引人的郵件務必停看聽！

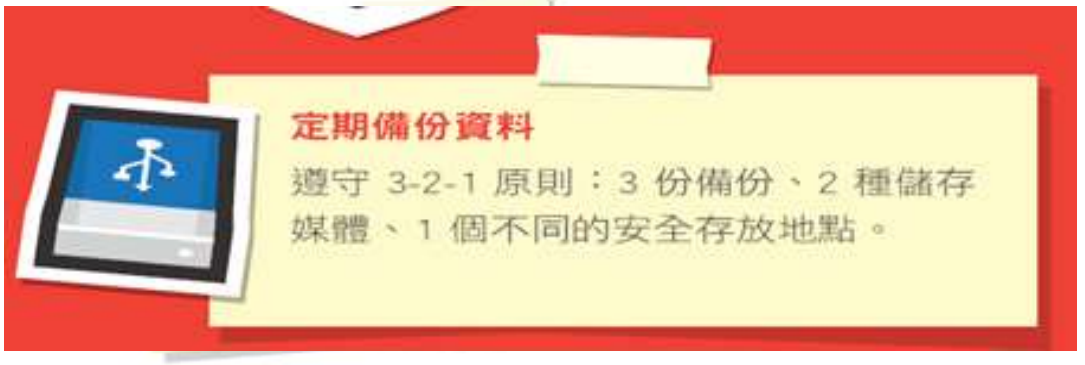
不打開:
不隨便打開email附件檔

不點擊:
不隨意點擊email夾帶的網址

要備份:
重要資料要備份

要確認:
開啟電子郵件前要確認寄件者身分

要更新:
病毒碼一定要隨時更新



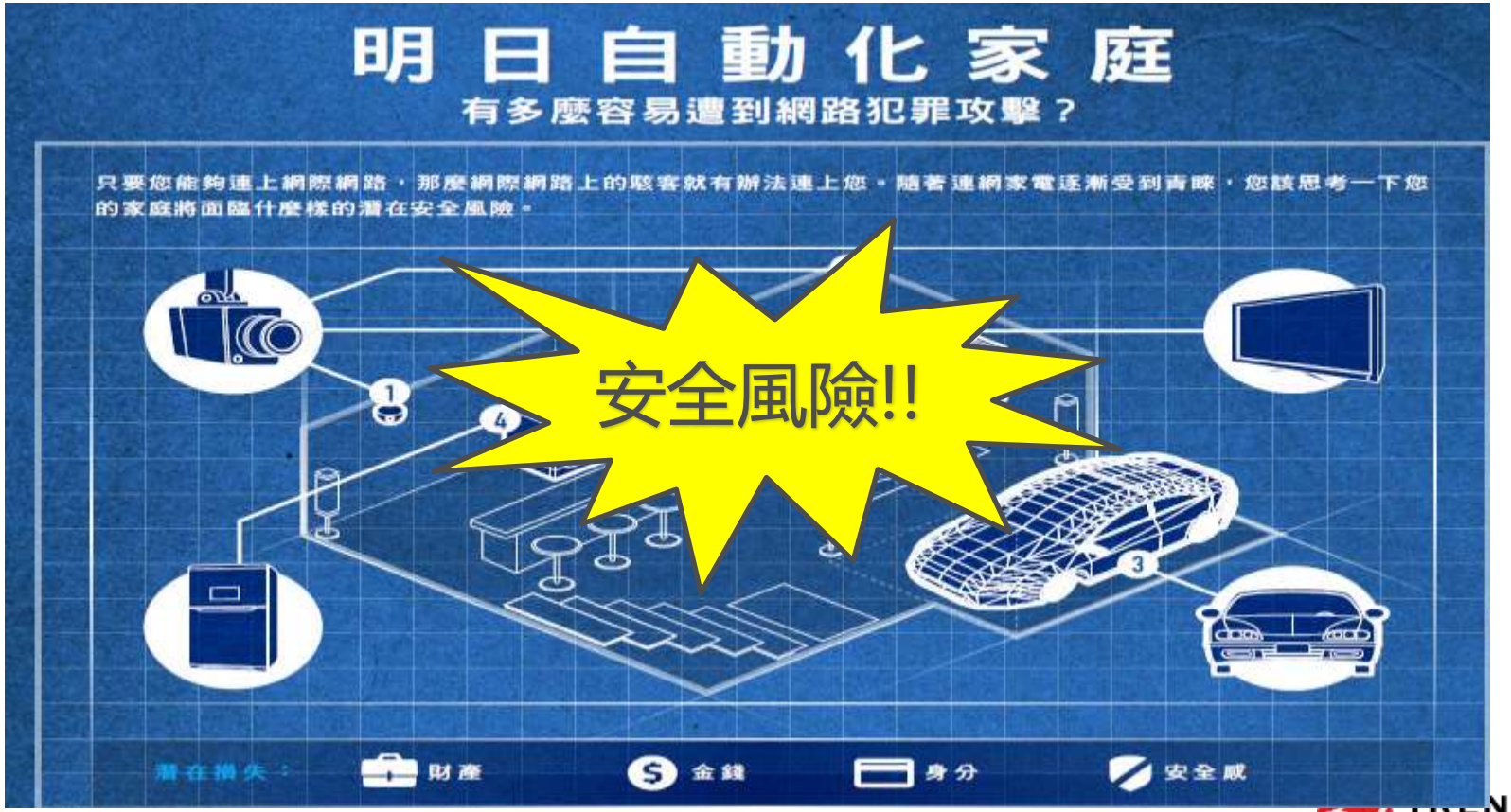
IOE萬物聯網

IOE (Internet of Everything) 萬物聯網

- IOE是近年最盛行的科技流行語
  - 任何新科技產品在設計時都會考慮到連接性
  - 智慧型電視
  - 智慧型烤麵包機
  - 汽車
  - 嬰兒監視器

TREND MICRO

IOE萬物聯網


明日自動化家庭
有多麼容易遭到網路犯罪攻擊？
只要您能夠連上網際網路，那麼網際網路上的駭客就有辦法連上您。隨著連網家電逐漸受到青睞，您該思考一下您的家庭將面臨什麼樣的潛在安全風險。
安全風險!!
1
2
3
4
潛在損失：
財產
金錢
身分
安全感

IOE萬物聯網

❶監視攝影機、動作感應器、門鎖、保全裝置

優點：

家庭保全系統可自動將窗戶和出入口上鎖來保障家庭安全。此外，更搭配警報系統與監視攝影機來防止歹徒入侵。當保全系統連上網際網路時，屋主就能從遠端直接遙控管理。

缺點：

連上網際網路的保全系統有可能遭到駭客入侵。

萬一遭到駭客入侵：

網路犯罪者若能從網際網路進入您的保全系統，就能掌握您不在家的時間以便闖空門，此外，必要時還能隨時關閉您的保全系統。

❷智慧型電視

優點：

內建攝影機和麥克風的智慧型電視可具備臉部辨識和語音辨識功能，如此就能針對不同的使用者與使用時機套用專屬設定。

缺點：

網路犯罪者可能入侵連網的智慧型電視並暗中操控它來錄下您的活動影像或聲音。

萬一遭到駭客入侵：

您可能哪天會突然發現自己和家人的影片被人上傳到不當的網站。此外，網路犯罪者還可能會利用智慧型電視所拍攝的影片或照片來竊取您的身分或向您勒贖。

TREND MICRO

IOE萬物聯網

❸ 汽車

優點：

車用電腦系統可讓您將某些重要的系統設定自動化，包括馬力、煞車、定速巡航。

缺點：

網路犯罪者若能透過一些網際網路服務（如影音串流、導航或網頁瀏覽）入侵車用電腦系統，即可對您車子的功能動手腳，並且/或者追蹤您車輛的定位資訊。

萬一遭到駭客入侵：

如果網路犯罪者讓您的煞車失靈，您將陷入嚴重的危險當中。

❹ 智慧型冰箱

優點：

智慧型冰箱可讓您透過 LCD 螢幕在線上採購日用品，某些機種還能協助您遵從飲食計劃，根據已儲存選單來追蹤食物的存量。

缺點：

網路犯罪者可能竊取您線上採購日用品的登入資訊，冒用您的名義購買一些不是您要的東西。

萬一遭到駭客入侵：

您可能得支付一些您從未訂購的日用品。

保護IOE萬物聯網

- 定期更新產品韌體
  - 任何系統都會有缺陷或漏洞，也因為如此，廠商會釋出韌體更新來在此情況下修補其萬物聯網設備。

- 保護網路
  - 任何連到家庭網路的設備都必須具備安全和防護入侵的能力。

    eg:防火牆

TREND MICRO

網絡安全需知

- 使用正版軟件。
- 安裝電腦防護方案，並確保其運作並定期更新，定期用防毒軟件掃描電腦。
- 採用如網頁信譽評分服務(Web reputation)。
- 安裝、更新和開啟防火牆、入侵偵測系統。
- 不要下載來源或性質可疑的軟件。

網絡安全需知

- 更新軟件 & plug-in。
- Window: 請啟動自動更新功能並執行更新的安裝內容。

- 詳讀用戶授權合約; 除了所需要的軟件外,還有其他程式將一起被安裝的話，請取消安裝程序。

社交媒體保安

- 避免於不同的平台使用同一個密碼
- 設定妥當密碼，並定期更改
- 更新智能電話的系統及應用程式 (App)，包括社交媒體的應用程式
- 金錢交易、購買點數卡或充值卡時，必須核實對方身份及該項要求的真確性 (By call)



無憂無慮享受數碼生活



THANK YOU

更多資料：trendmicro.com.hk