

# 瞭解駭客攻擊，就不用怕駭客 2011電腦病毒發展趨勢

By  
Diamond Liu 劉得民  
(a.k.a. Jamien Liu 劉楨民)

Malware vs. Anti-Malware

My first wish is to see this plague of mankind, war, banished from the earth.

George Washington, 1st US President

# 瞭解駭客攻擊，就不用怕駭客

- 駭客社交工程的特性說明
- 個人電腦感染病毒的主要來源
- 親友電郵遭駭 詐騙匯款
- 即時通病毒蠕蟲 詐騙親友匯款
- 下載來路不明檔案 網路銀行遭盜領
- Facebook的隱藏憂慮
  - USB 隨身碟的資安防範
  - 網路安全的基本防護方式
  - 網路安全的 資安五要
- Q&A

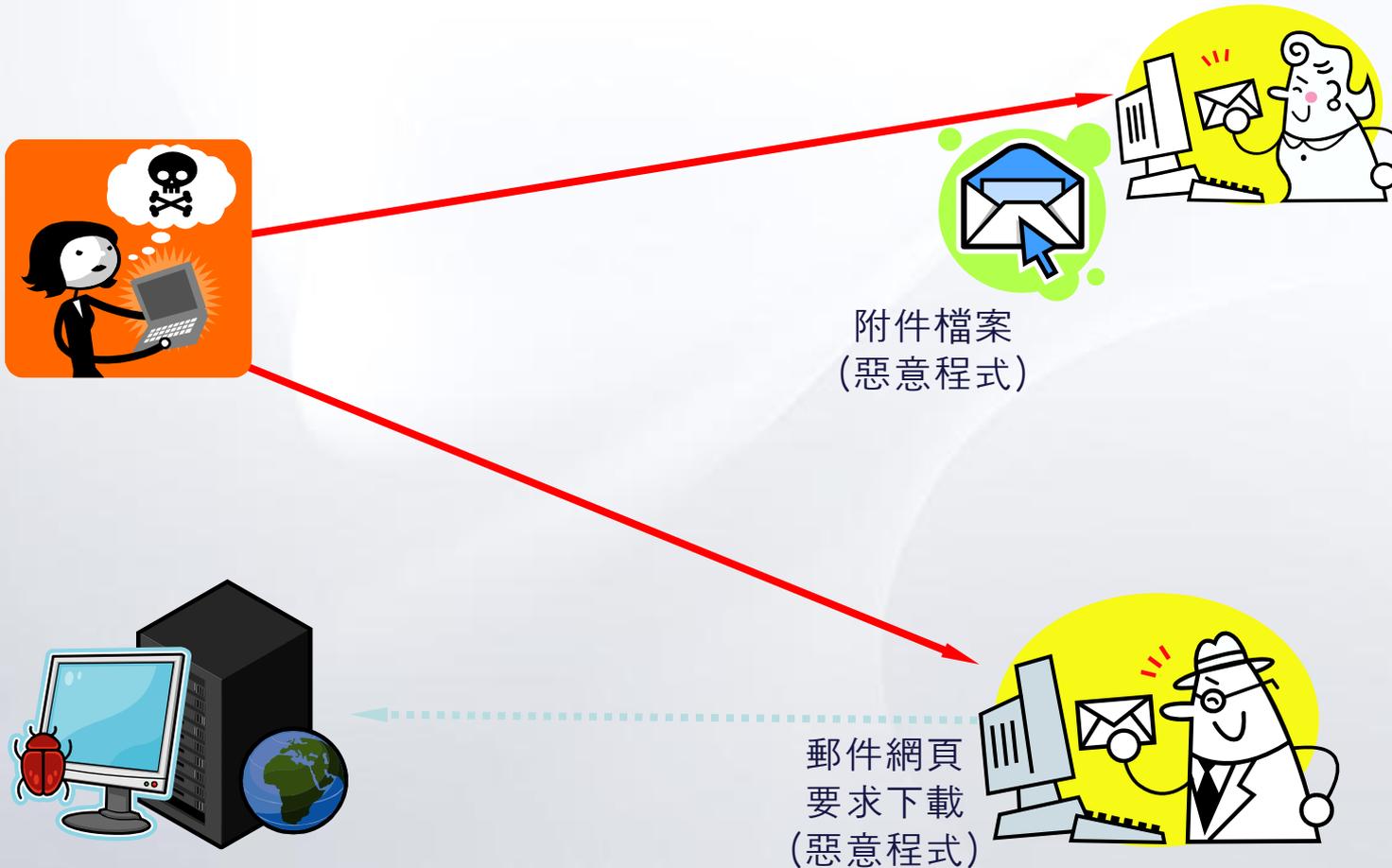
# 駭客社交工程的特性說明

- 駭客社交工程攻擊 Social Engineering
- 資訊安全保護的三個目標
  - 保護資訊 (I, information)
  - 保護資源 (R, resource)
  - 保護隱密性 (P, privacy)
- 資訊安全的基礎是**制度**不是**信任**
- 駭客社交工程，會取得被害人的信任，並透過自己認識的親友進行駭客攻擊！

# 個人電腦感染病毒的主要來源-1

## 1. 透過電子郵件傳送感染

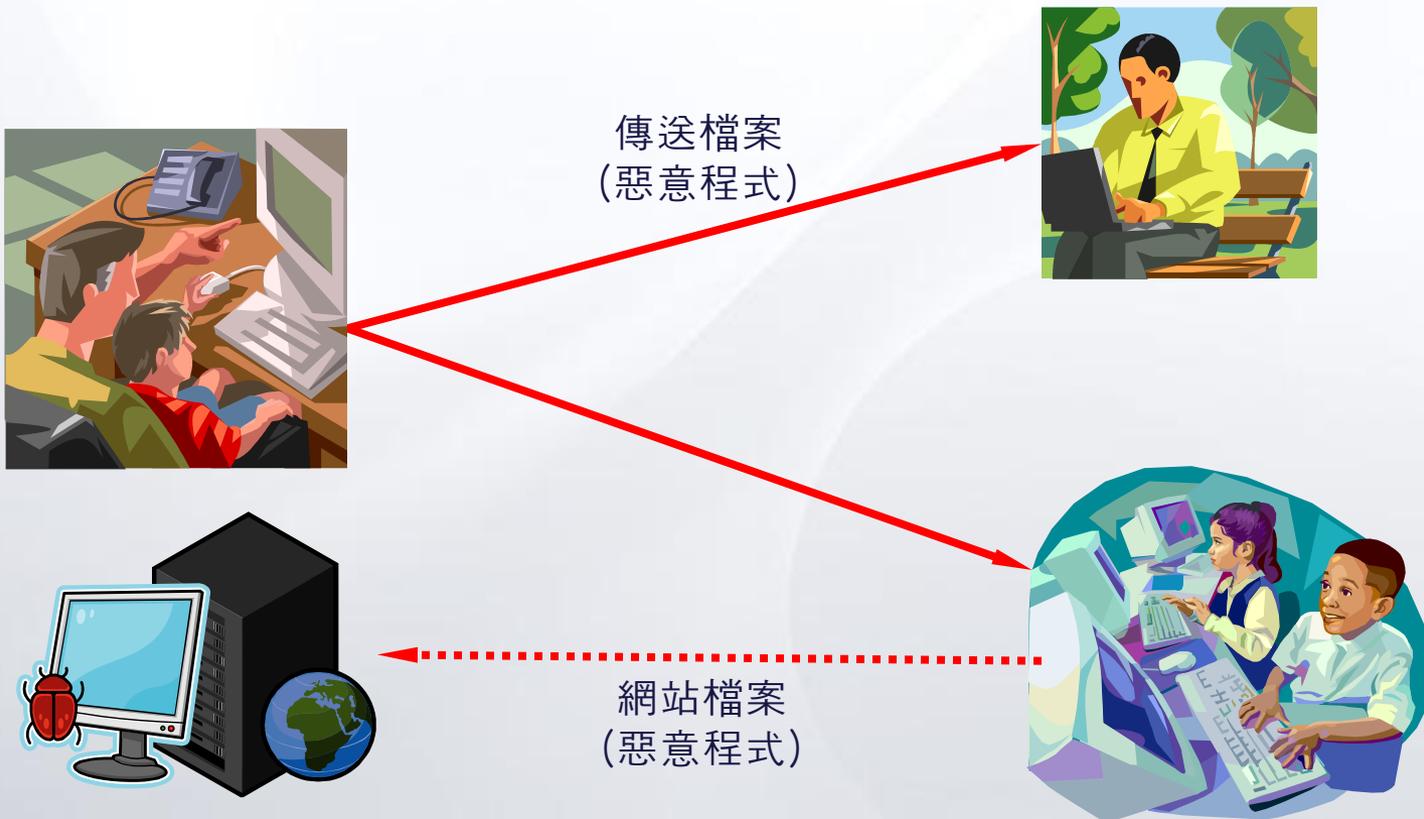
- 附件檔案 包含病毒木馬檔案
- 郵件網頁 要求下載安裝檔案



# 個人電腦感染病毒的主要來源-2

## 2. 即時通 與 網頁瀏覽

- 點選網頁超連結 要求下載安裝惡意檔案
- 即時通用戶傳送病毒檔案 (已經不多見, 烤雞病毒)

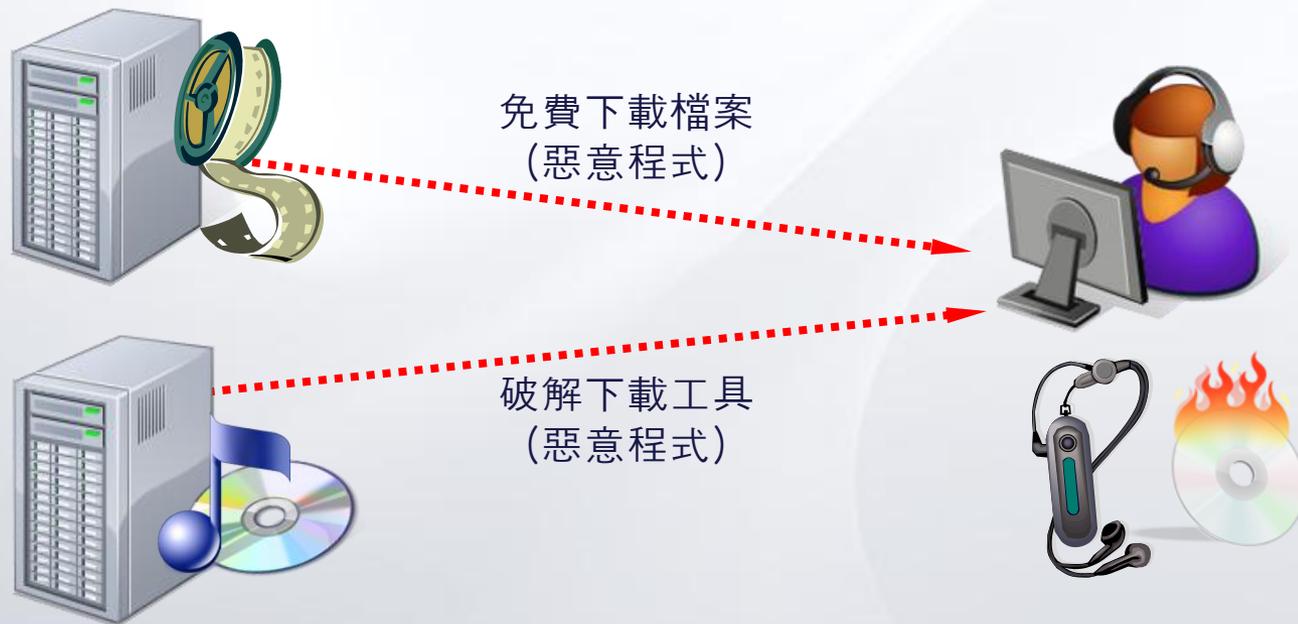


# 個人電腦感染病毒的主要來源-3

## 3. 下載軟體

- 免費工具，盜版軟體
- 好玩遊戲，可愛圖案，螢幕保護程式

註：USB 隨身碟與USB拇指碟（它們只是傳播媒介，類似蒼蠅與蚊蟲，不是真正病毒來源）



# 親友電郵遭駭 真實案例

## 假冒指導教授發出電郵 大學講師匯款被騙

某大學講師接到以前指導教授的求助電子郵件，內容為老師在國外需要金錢幫助。該名講師隨即按照指示匯了2,800美金到英國，事後才得知老師在國內。

被冒名的教授，曾接到冒充信箱管理員確認帳號的電子郵件，填了相關資料之後不僅資料外洩，電子信箱也一整天都無法使用。

歹徒經由釣魚手法取得這名教授的通訊錄之後，假冒名義向學生發出借錢e-mail，詐騙得逞。



用戶端  
被植入  
惡意程式



駭客

向親友散佈  
虛假訊息

竊取  
電郵  
通訊錄



電郵詐騙匯款



# 親友電郵遭駭 真實案例

## 假藉Facebook名義 入侵電腦

熱門的社群交友機制, Facebook, 許多人都有在其中種菜養魚的經驗, 最近有電子郵件假借Facebook帳號通知的名義, 該電郵信件內容(中英文皆有): 為了確保帳號安全, 要求用戶重新設定Facebook帳號。

若是使用者若想要知道其重新設定的帳號, 就必須先開啟郵件中的附件檔案, 來誘使Facebook使用者開啟郵件中夾帶檔案。而實際上這個附件檔中隱藏了一個名為「Trojan Bredolab」的木馬程式。



# 親友電郵遭駭 真實案例

## 假藉Facebook名義 入侵電腦

熱門的社群交友機  
菜養魚的經驗，最  
知的名義，該電郵  
帳號安全，要求用

若是使用者若想要  
開啟郵件中的附件  
郵件中夾帶檔案。  
名為「Trojan Bre

The Facebook Team

To:

📎 Facebook\_Password\_7a343.zip (23.8 KB)

Facebook Password Reset Confirmation.

Hey ,

Because of the measures taken to provide safety to our clients, your password has been changed.

You can find your new password in attached document.

Thanks,

The Facebook Team

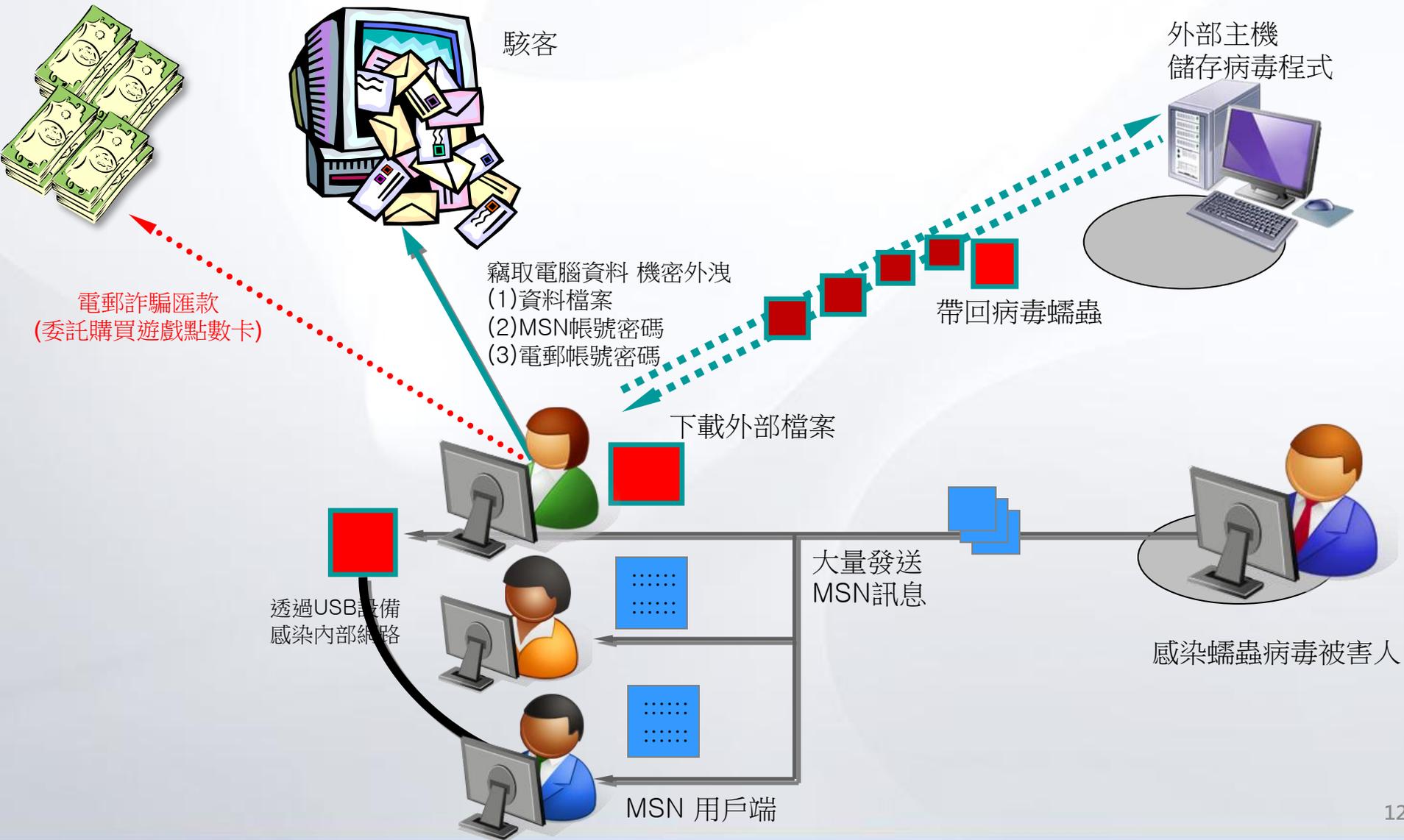
The message comes with a .zip file containing a malicious Trojan.Bredolab.

This variant of Bredolab connects to a Russian domain and the infected botnet.

# 加入好友清單



# 即時通病毒蠕蟲 詐騙親友匯款



# 你看得出來，誰有問題嗎？

<input type="checkbox"/>	!	新	dmliu@ms4.hine...	[X-Span]RE: Pharmacy Message 11304	02/11 17:18	2K
<input type="checkbox"/>		新	The Code Proje...	[CodeProject] Daily News - Get a free domain...	02/11 13:11	15K
<input type="checkbox"/>			United Mileage...	My Mileage Plus Summary - February 2009	02/10 20:58	30K
<input type="checkbox"/>			何	^__^你嚇到他了!!!	02/09 14:12	221K
<input type="checkbox"/>			楊林森	Fw: (有關資訊安全)請檢查一下自己的電腦有沒有不...	02/09 11:10	2K
<input type="checkbox"/>			001051kimo	知道什麼叫做邊鞦韆嗎？	02/09 10:50	6K
<input type="checkbox"/>			Intel (R) Soft...	英特尔(R) C++ 編譯器 Windows* 专业版 评估版到期通...	02/09 00:04	4K
<input type="checkbox"/>			"Anshuman Prat...	RE: RE: RE: Partnership for Taiwan	02/06 17:56	119K
<input type="checkbox"/>			The Code Proje...	[CodeProject] Daily News - The case for supp...	02/06 16:06	15K
<input type="checkbox"/>			Intel Performa...	Survey reminder: Intel® IPP Evaluation Vers...	02/06 13:20	3K
<input type="checkbox"/>			台北市電腦公會	TCA會訊--2009台北國際電玩展，2/12-...	02/05 17:23	25K
<input type="checkbox"/>			The Code Proje...	[CodeProject] Daily News - The power of pers...	02/05 13:07	15K
<input type="checkbox"/>			Rossy 龔綺雲	Fw: Micro net	02/04 14:51	2K
<input type="checkbox"/>			intel.software...	Intel® Evaluation Survey: Intel C++ Compile...	02/03 21:35	4K
<input type="checkbox"/>	!		Richy Huang	合作:採購重要資訊通知-廣得利貿...	02/02 11:13	450K
<input type="checkbox"/>			何	~~~sorry~~~	01/31 23:58	230K
<input type="checkbox"/>			何	迷你女郎圖片	01/31 18:09	6K
<input type="checkbox"/>			001051kimo	在無名上看到的 現在的年輕人阿	01/26 07:07	221K
<input type="checkbox"/>			001051kimo	安安.....	01/25 14:39	6K
<input type="checkbox"/>			云貞黃	朋友就要像你這樣的...	01/25 03:42	5K
<input type="checkbox"/>			001051kimo	真滴很麻煩你勒~~太需要你的幫忙...	01/25 01:21	6K
<input type="checkbox"/>			st.huang	我瘦下來啦...趕緊告訴妳小撇步	01/24 19:30	192K

何 ~~~sorry~~~

001051kimo 安安.....

云貞黃 朋友就要像你這樣的...

001051kimo 真滴很麻煩你勒~~太需要你的幫忙...

st.huang 我瘦下來啦...趕緊告訴妳小撇步

何 ^\_\_^你嚇到他了!!!

何 迷你女郎圖片

001051kimo 在無名上看到的 現在的年輕人阿



照樣有毒!!



- 收件匣 (21)
- 垃圾郵件
- 草稿
- 寄件備份
- 刪除的郵件 (1)
- 管理資料夾
- 首頁
- 郵件
- 連絡人
- 行事曆
- 生活資訊 休閒娛樂 特價優惠

FW: (我是德明的王姿懿, 這是病毒信) [7 10急件] 我訂婚了

寄件者: Wendy (wendy76802@yahoo.com.tw)

寄件日期: 2008年8月2日 下午 03:55:41

回覆地址: wendy76802@yahoo.com.tw

收件者: dmliv99999@hotmail.com

@ 自拍婚紗.zip (202.3 KB)

下載時執行安全性掃描 TREND MICRO

--- 08/8/2 (星期六), 姿懿 <wendy520yaya@yahoo.com.tw> 寫道:

寄件者: Wendy (wendy520yaya@yahoo.com.tw)

主旨: FW: [7 10急件] 我訂婚了

收件者: Wendy (wendy76802@yahoo.com.tw)

日期: 2008 8 2 星期六 下午 11:50

Microsoft Internet Explorer

檔案 (自拍婚紗.zip) 受到未知病毒的感染，因此下載檔案是不安全的。

確定

--- 08/7/11 (星期五), 王姿懿 <wendy520123@yahoo.com.tw> 寫道:

寄件者: Wang Shan Chang (wsc510@yahoo.com.tw)

主旨: [7 10急件] 我訂婚了

收件者: Wendy (wendy520123@yahoo.com.tw)

日期: 2008 7 11 星期五 上午 3:18

7 10  
好久沒有聯絡了 我訂婚了 給我祝福吧 發張婚紗照給你 看看你能不能認出我  
7 10

總會某些時刻，突然想起舊情人？他現在過得還好嗎？ - 馬上搜尋！



- 收件匣 (21)
- 垃圾郵件
- 草稿
- 寄件備份
- 刪除的郵件 (1)
- 管理資料夾
- 首頁
- 郵件
- 連絡人
- 行事曆
- 生活資訊 休閒娛樂 特價優惠

新增 回覆 全部回覆 轉寄 刪除 垃圾郵件 置於資料夾 選項

FW: (我是德明的王姿懿, 這是病毒信) [6/27急件] 別了 朋友們

寄件者: Wendy (wendy76802@yahoo.com.tw)

寄件日期: 2008年8月2日 下午 03:55:17

回覆地址: wendy76802@yahoo.com.tw

收件者: dmliv99999@hotmail.com

@我的遺書.zip (173.8 KB)

下載時執行安全性掃描 TREND MICRO

--- 08/8/2 (星期六), 姿懿 <wendy520yaya@yahoo.com.tw> 寫道:

寄件者: wendy520yaya@yahoo.com.tw

主旨: FW: [6/27急件] 別了 朋友們

收件者: wendy76802@yahoo.com.tw

日期: 2008 6 2 星期六 下午 11:50

Microsoft Internet Explorer

檔案 (我的遺書.zip) 受到未知病毒的感染, 因此下載檔案是不安全的。

確定

--- 08/6/27 (星期五), cherylcusa@yahoo.com.tw <cherylcusa@yahoo.com.tw> 寫道:

寄件者: cherylcusa@yahoo.com.tw <cherylcusa@yahoo.com.tw>

主旨: [6/27急件] 別了 朋友們

收件者: wendy36200@yahoo.com.tw

日期: 2008 6 27 星期五 上午 4:44

6/27  
 這個世界已經沒什麼值得我眷戀了 永別了 朋友們  
 這是我給你們的訣別信  
 6/27

# 打字聊八卦，又慢又沒Fu



- 收件匣 (21)
- 垃圾郵件
- 草稿
- 寄件備份
- 刪除的郵件 (1)
- 管理資料夾
- 首頁
- 郵件
- 連絡人
- 行事曆

新增 回覆 全部回覆 轉寄 刪除 垃圾郵件 置於資料夾 選項

FW: (我是德明的王姿懿, 這是病毒信) 想找新工作

寄件者: Y姿 (wendy76802@yahoo.com.tw)  
 寄件日期: 2008年8月2日 下午 03:47:37  
 回覆地址: wendy76802@yahoo.com.tw  
 收件者: dmliv99999@hotmail.com  
 @讚讚讚--拜託拉!...zip (98.3 KB)

下載時執行安全性掃描 TREND MICRO

-- 08/11/12 (星期六), <chi19880316@yahoo.com.tw> 寫道

寄件者: 張綺綺 <chi19880316@yahoo.com.tw>  
 主旨: 想找新工作  
 收件者: s81750@yahoo.com.tw, mei900420@yahoo.com.tw, a\_tzu\_1020@yahoo.com.tw, wendy76802@yahoo.com.tw, rita01230@yahoo.com.tw, w9034834@yahoo.com.tw, ruby198710302000@yahoo.com.tw, g90238@yahoo.com.tw, c22631030@yahoo.com.tw, alexmax234@yahoo.com.tw, clse0359@yahoo.com.tw, winnie33k@yahoo.com.tw, jackson29449935@yahoo.com.tw, kyo76823@yahoo.com.tw, lovehu1013@yahoo.com.tw, s22616227@yahoo.com.tw, saysa@yahoo.com.tw, turtle90332@yahoo.com.tw  
 日期: 2008 7 12 星期六 上午 3:00

親愛的朋友好久不見---我想換工作了如果有甚麼好工作徵人可以幫我留意  
 總會在某些時刻, 突然想起舊情人? 他 現在過得還好嗎? - [馬上搜尋!](#)  
 總會在某些時刻, 突然想起舊情人? 他 現在過得還好嗎? - [馬上搜尋!](#)

### 檔案下載

是否要開啓或儲存這個檔案?

名稱: 讚讚讚--拜託拉![1]..zip  
 類型: WinRAR ZIP archive, 126 KB  
 來自: 65.55.172.39

開啓(O) 儲存(S) 取消

雖然來自網際網路的檔案可能是有用的, 但是某些檔案有可能會傷害您的電腦。如果您不信任其來源, 請不要開啓或儲存這個檔案。有什麼樣的風險?

dmliu 您好，您的(收件匣)共有 1823 封信。

寫新信

查詢信件： 依主旨查詢 [ ] GO

信件匣 [管理]

收件匣 >>

草稿匣

寄件備份

垃圾桶 [清空]

垃圾信件匣 [清空]

我的信件匣

我的同事

我的同學

我的家人

我的朋友

外部信箱

個人設定

線上輔導

刪除 轉寄 垃圾信 搬移至...

▼	!	📧	寄件者	主旨	日期 ▼	大小
<input type="checkbox"/>			新波科技_周芋...	3/27 芋玲業務連絡事項	08/27 18:22	6K
<input type="checkbox"/>			<b>新波科技_周芋...</b>	<b>Re: APacketMan國中小版本-功能需求(我有寄給您呀!)</b>	<b>04/07 16:38</b>	<b>4K</b>
<input type="checkbox"/>		📧	王瑞材	台北科技大學電子系_專題學術演講通告(970411)	04/07 15:17	148K
<input type="checkbox"/>			新波科技_周芋...	4/24 國防部 上課題目【網路安全威脅與駭客入侵】	04/07 13:32	3K
<input type="checkbox"/>			新波科技_周芋...	Fw: 4/15研習_中平國中_木馬後門與網路管理的愛恨...	04/07 13:24	1K
<input type="checkbox"/>			新波科技_周芋...	Re: 劉植民老師演講照片	04/07 11:00	11K
<input type="checkbox"/>		📧	張念	性感女星衛生間大秀身材(組圖)	04/07 10:23	290K
<input type="checkbox"/>			陳 翊榮	演講邀請	04/07 00:51	2K
<input type="checkbox"/>			陳 翊榮	演講邀請	04/06 22:27	2K
<input type="checkbox"/>	!		廖鴻圖	麻煩協助講座	04/06 17:35	6K
<input type="checkbox"/>			KC2008論文組	2008知識社群與系統發展研討會 論...	04/06 16:47	2K
<input type="checkbox"/>			KC2008論文組	2008知識社群與系統發展研討會 論...	04/06 16:43	2K
<input type="checkbox"/>			Home Teitung...	台大資訊系大二生想到你那實習	04/06 04:40	2K
<input type="checkbox"/>		📧	oammmr...	給我背	04/06 00:16	392K
<input type="checkbox"/>			yuling.chou@ms...	請給我網管辣妹_MSN的病毒檔案	04/05 23:02	1K
<input type="checkbox"/>		📧	a90105kimo	吳上尉的木馬及病毒來啦	04/05 15:56	1M
<input type="checkbox"/>	!	📧	廖鴻圖	Re:KC2008知識社群與系統發展研討會-徵稿延期通知(4...	04/03 21:52	390K
<input type="checkbox"/>			yuling.chou@ms...	Re: Re: 20080403_用戶端資安觀念宣導-駭客社交工程...	04/03 21:30	14K
<input type="checkbox"/>		📧	新波科技_周芋...	新波科技向臺灣新媒體雜誌約 寄信未寄出	04/03 17:43	22K

最有保障的融資週轉管道 55歲學英文4週通過英檢 數位娛樂新世界

網頁郵件 通訊錄 贈品索取 成功貸款

現在位置：網頁郵件 > 讀信

## 讀取信件

WEB MAIL @ HINET 登出

→ 搬移至...

展開功能列

回信 全部回信 轉寄 檢視信件原始檔 友善列印 下載信件 刪除

dmliu: 收件匣

上一封 | 下一封 | 返回

寄件人：張念 <cmiscc23058@yahoo.com.tw> 加入通訊錄 檢舉垃圾信

收信人：chung6391@pchome.com.tw, clean740807 <clean740807@yahoo.com.tw>, cmiscc23058@yahoo.com.tw, conny <conny12122002@yahoo.com.tw>, cobi.suzy@ching-win.com.tw, coupe455 <coupe455@yahoo.com.tw>, d3kvik@yahoo.com.tw, diskcard@msa.hinet.net, dj94xk48 <dj94xk48@yahoo.com.tw>, dmlin@ms4.hinet.net,

日期：Mon, 7 Apr 2008 10:23:14 +0800 (CST)

主旨：性感女星衛生間大秀身材(組圖)

附檔：@性感女星(組圖)12張.rar(154K)

@玫瑰.GIF(59.8K)

甚麼是 衛生間？ 廁所是也！ 此為 老共用語！

※推論1：使用台灣專用的繁體中文，該病毒為老共專門為台灣調製的木馬

※推論2：區域病毒(Local Virus)，國際掃毒軟體找得到它嗎？

※再次說明，掃毒軟體告訴妳：電腦沒有中毒。

**只代表它沒有掃到毒，不表示電腦檔案是乾淨的環境！**



科技 CEO 防毒 欺騙

Google 搜尋

好手氣

[ZDNet Taiwan - 趨勢CEO陳怡樺：防毒產業騙了客戶20年- 新聞- 企業 ...](#) 🔍

[www.zdnet.com.tw/news/.../0,2000085678,20130359,00.htm](#) - 頁庫存檔

2008年7月2日 - 趨勢科技 (Trend Micro) 執行長陳怡樺對於防毒產業過去20年來的效能有一番 ... 在防毒產業，我們已經騙了客戶20年了，大家都以為防毒軟體可保護 ...

[誰騙了你20年@ 就是資安:: 痞客邦PIXNET ::](#) 🔍

[cyrilwang.pixnet.net/blog/post/25637117-誰騙了你20年](#) - 頁庫存檔

這一陣子，有一個還算蠻震撼的新聞，就是趨勢科技的CEO陳怡樺說了「防毒產業騙了客戶20年」這麼一句話。這一句話，不但打翻了趨勢科技自己一直以來的產品，也 ...

[謬打誤撞的驚人發現~~~~~防毒產業騙了客戶20年!!!!](#) 🔍

[www.wretch.cc/blog/lf260703/24269005](#) - 頁庫存檔

2010年11月1日 - 看到一篇趨勢科技CEO一篇爆炸性發言：防毒產業騙了客戶20年，可是讓我好奇不已，看完整篇新聞卻有種莫名的情感交織，轉貼重點如下： ...

[趨勢CEO陳怡樺：防毒產業騙了客戶20年- iT邦幫忙::IT知識分享社群](#) 🔍

[ithelp.ithome.com.tw/question/10005614](#) - 頁庫存檔

23 個答案 - 2008年7月3日

趨勢科技 (Trend Micro) 執行長陳怡樺對於防毒產業過去20年來的效能有一番 ... 在防毒產業，我們已經騙了客戶20年了，大家都以為防毒軟體可保護 ...

在防毒產業，我們已經騙了客戶20年了，  
大家都以為防毒軟體可保護他們，  
但其實我們不可能完全擋住病毒。

[年@ 網路暨遊戲安全防護哈拉板 ...](#) 🔍

於防毒產業過去20年來的效能有一番 ...  
防毒軟體可保護 ...

寄件者	主旨
Home Taitung	地震天母房子如何
Tofer	型錄
朱璟淳	NII課程測驗題-請老師提供
Tofer	s-monitor 進度
SearchSecurity...	Expert guidance on app layer security; com
姿汶	公司的系統欄位-MONICA
The Code Proje...	[CodeProject] Daily News - The top 3 clo
RFID基礎應用技...	RFID 晶片設計教師研習會【歡迎參...
Mike	祝您今年虎虎生威阿~
a90105kimo	網咖剛認識的美眉.
a90105kimo	愛情測試.副件密碼520
a90105kimo	男士請進.MM勿入.嘿嘿~~副件密碼6
Advanser	迎春納福.前展顧問祝大家虎年行大運發
張國	Re: 關於 Diamond group meeting 2月20日
逸凡科技行銷部	逸凡科技陳逸文跟 您拜年!
張國	Re: 關於 Diamond group meeting
Mike	謝謝各位百忙之中抽空前往!!
宋茂深	請教找木馬病毒之DOS指令
林啟瑞	RE: 很榮幸今天能與您見到面~
Mike	Fw: 很榮幸今天能與您見到面~
Mike	Re: 很榮幸今天能與您見到面~
新波科技	FW: 資安研討會主題及大綱

主旨：網咖剛認識的美眉.

附檔： @網咖剛認識的美眉.rar(81.1K)

前幾天去網咖新認識的美眉....長的像不像明星黃聖依~~副件密碼520

02/25 09:38 450K

主旨：愛情測試.副件密碼520

附檔： @愛情測試.rar(81.3K)

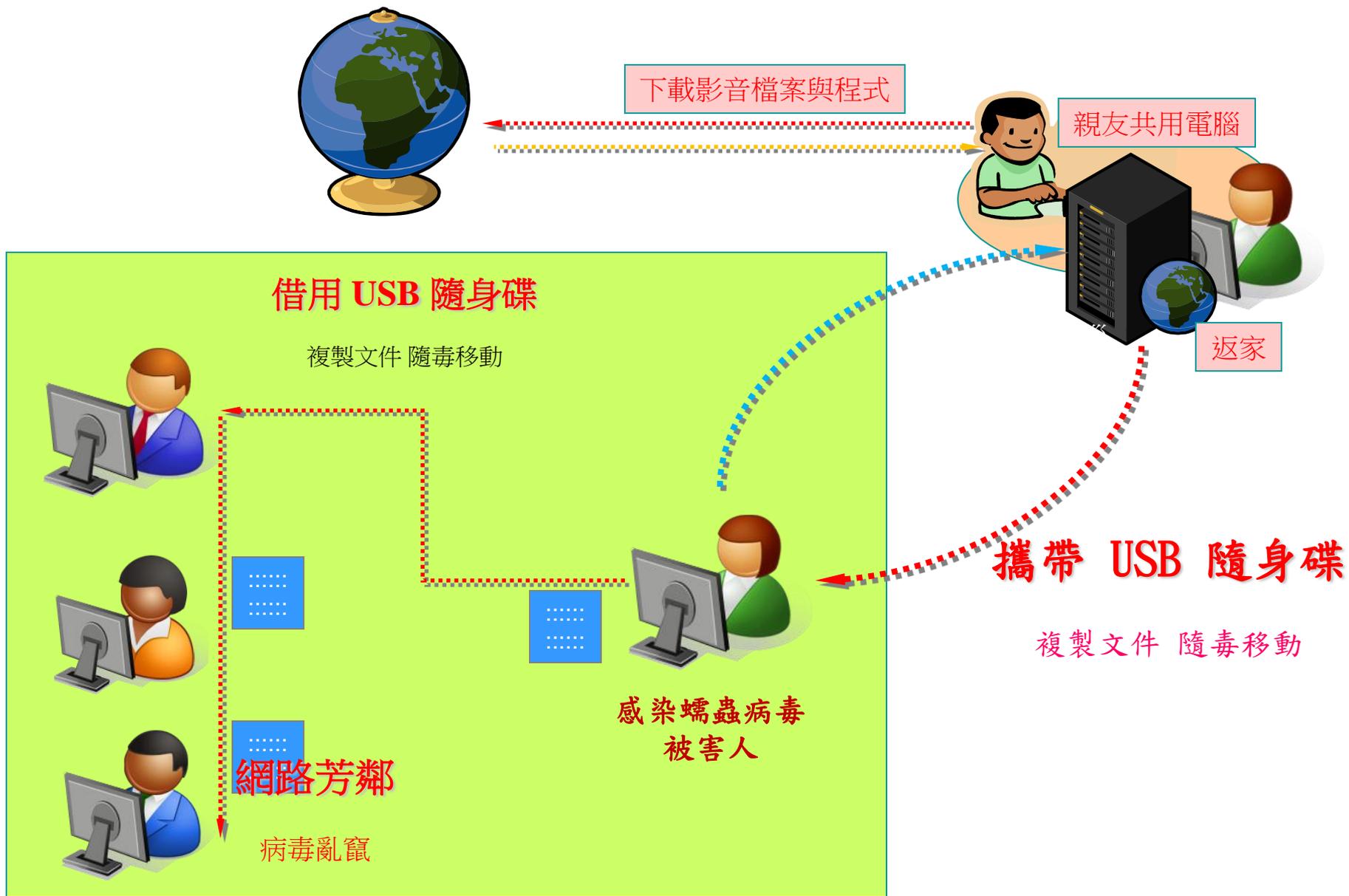
測試下你們愛情是不是能地老天荒.讓你了解對方....更能了解自己.....

主旨：男士請進.MM勿入.嘿嘿~~副件密碼668

附檔： @男士請進.MM勿入.嘿嘿.rar(81.1K)

如果你淪落到一個荒島上.你會選擇那條魚....看帖就要回哦.不回後果自負!!!!

# 私人電腦 與 學校電腦 的交互感染



# USB 隨身碟的資安防範

USB儲存設備感染病毒後，不容易清除，因為…

1. 隨身碟，拇指碟，MP3播放器，手機，數位相機，記憶卡等等都可能已經感染 USB病毒，到處傳染其他電腦。

2. 常見USB儲存設備病毒有兩種，

A. 自動執行方式 → Autorun.inf (容易對付)

B. 隱藏文件方式 → 正式文件.doc.exe 或是 目錄名稱.exe



# 看得出來？這個USB-F碟，有毒嗎？

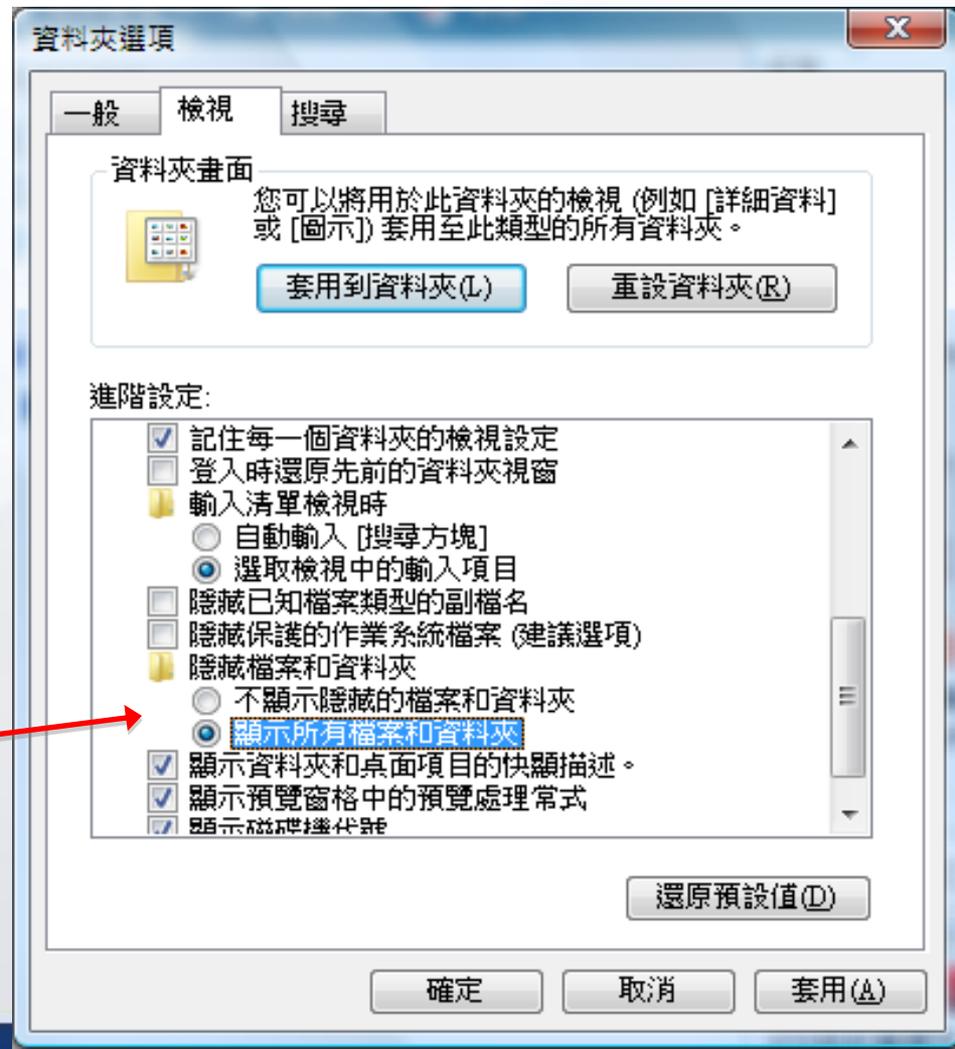
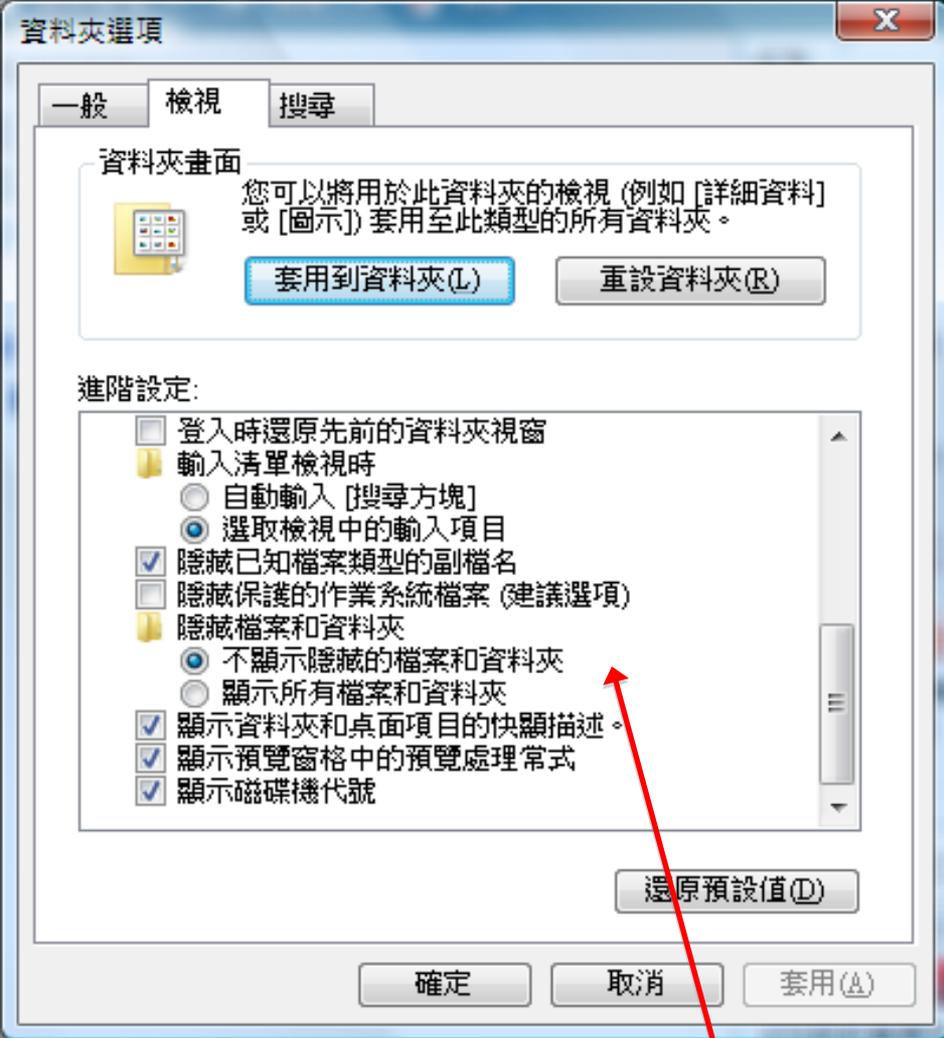
最愛連結

- 文件
- 圖片
- 音樂
- 其他 >>

資料夾

- 桌面
- dmliu
- 公用
- 電腦
- VistaOS (C:)
- DATA (D:)
- DVD RW 磁碟機 (E:)
- USB (F:)
- BD-ROM 光碟機 (H:)
- 網路
- 控制台
- 資源回收筒
- GodMode.{ED7BA470-8E54-465E-825C-99712C}

名稱	修改日期	類型	大小	標記
.fseventsd		Folder		
.Spotlight-V100		Folder		
.Trashes		Folder		
2010-AAA		Folder		有性關係嘗試 - 嘗試評估 1. 進行性關係嘗試前 2. 進行性關係嘗試前 3. 進行性關係嘗試前 4. 進行性關係嘗試前 5. 進行性關係嘗試前 6. 進行性關係嘗試前 7. 進行性關係嘗試前 8. 進行性關係嘗試前 9. 進行性關係嘗試前 10. 進行性關係嘗試前
2010-即時題庫系統-流程圖		Diagram		
2011-04-02		Folder		
2011-04-16		Folder		
20110411-Online		Folder		
iOS設計基礎文件		PDF		
iPhone程式設計-0		PDF		
My Ling		Folder		
The Yuling in Report		Folder		



親愛的連結

- 文件
- 圖片
- 音樂
- 其他 >>

資料夾

- 桌面
- dmliu
- 公用
- 電腦
- VistaOS (C:)
- DATA (D:)
- DVD RW 磁碟機 (E:)
- USB (F:)
- BD-ROM 光碟機 (H:)
- 網路
- 控制台
- 資源回收筒
- GodMode.{ED7BA470-8E54-465E-825C-99712C}

名稱	修改日期	類型	大小	標記
.fseventsd		Folder		
.Spotlight-V100		Folder		
.Trashes		Folder		
2010-AAA		Folder		2010-AAA
2010-即時題庫系統-流程圖		Diagram		
2011-04-02		Folder		
2011-04-16		Folder		
20110411-Online		Folder		
iOS設計基礎文件		PDF		
iPhone程式設計-0		PPT		
My Ling		Folder		
The Yuling in		Folder		

名稱	修改日期	類型	大小	標記
.fseventsd.exe		Folder		
.Spotlight-V100...		Folder		
.Trashes.exe		Folder		
2010-AAA.ppt		Folder		2010-AAA.ppt
2010-即時題庫系統-流程圖.pptx		Diagram		
2011-04-02.exe		Folder		
2011-04-16.exe		Folder		
20110411-Online...		Folder		
iOS設計基礎文件.pdf		PDF		
iPhone程式設計-0.ppt		PPT		
My Ling.exe		Folder		
The Yuling in Report.exe		Folder		

最近的使用

- 文件
- 圖片
- 音樂
- 其他 >>

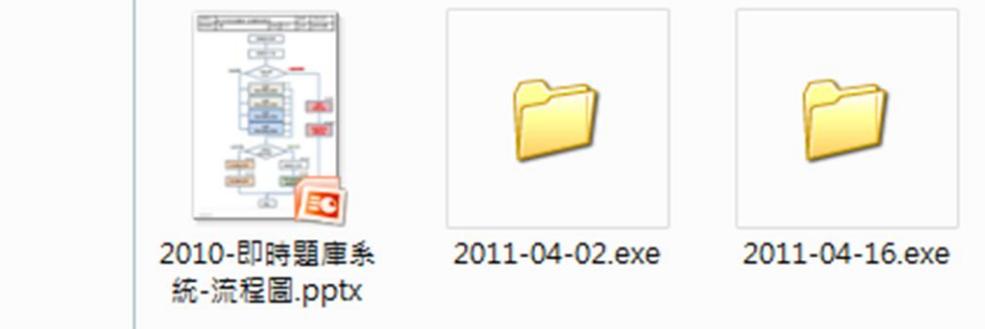
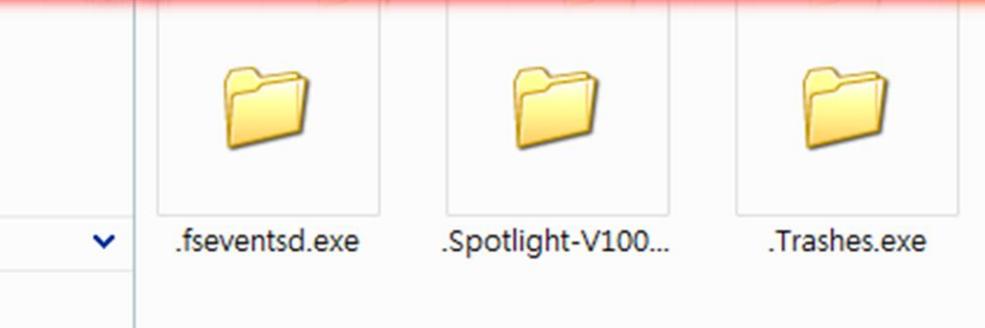
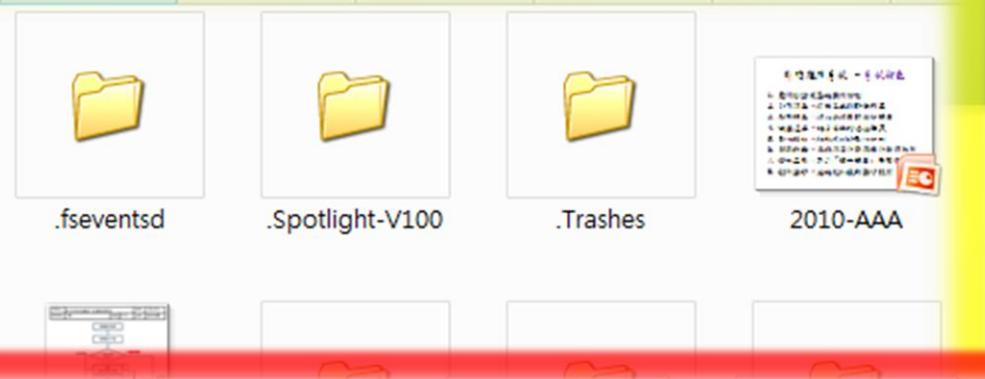
資料夾

- 桌面
- dmliu
- 公用
- 文件
- 圖片
- 音樂
- 其他 >>

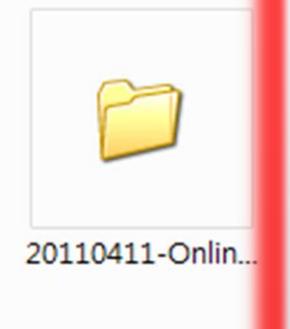
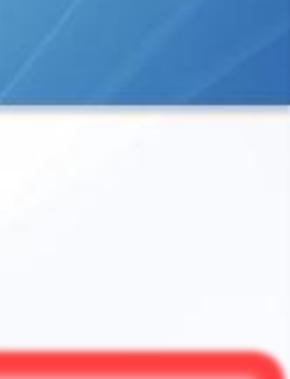
資料夾

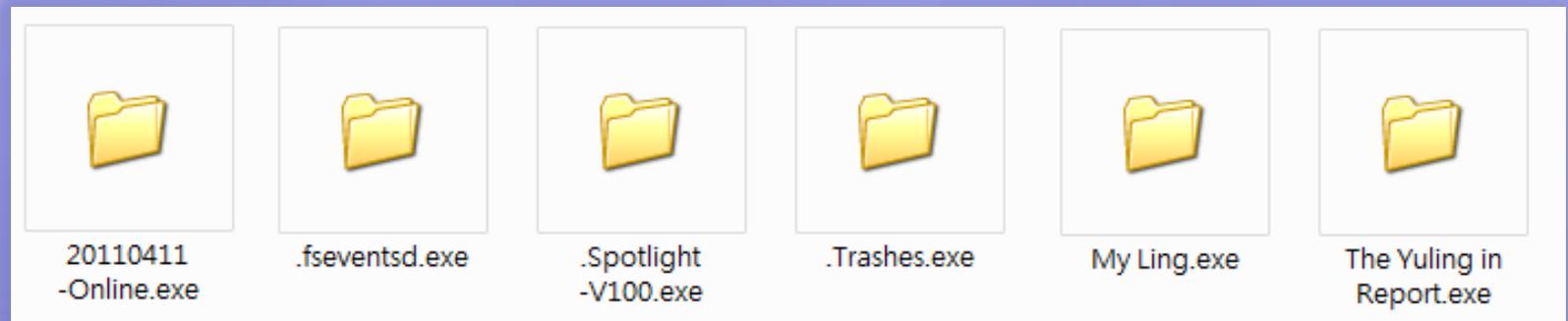
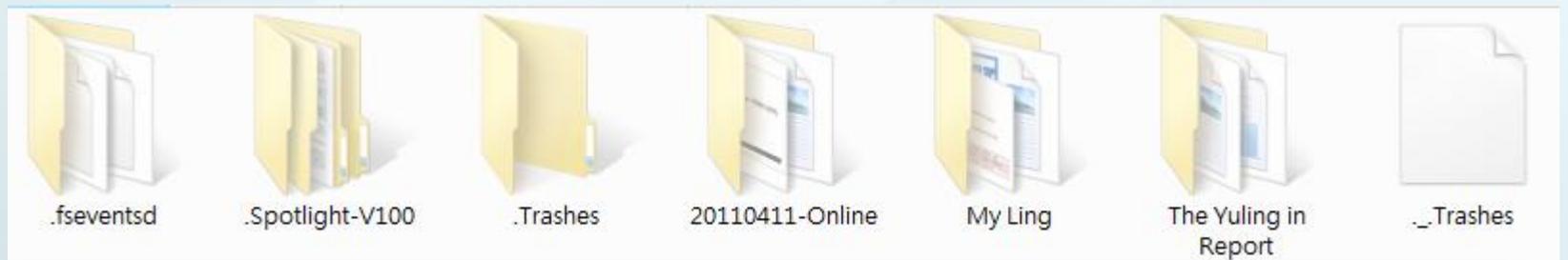
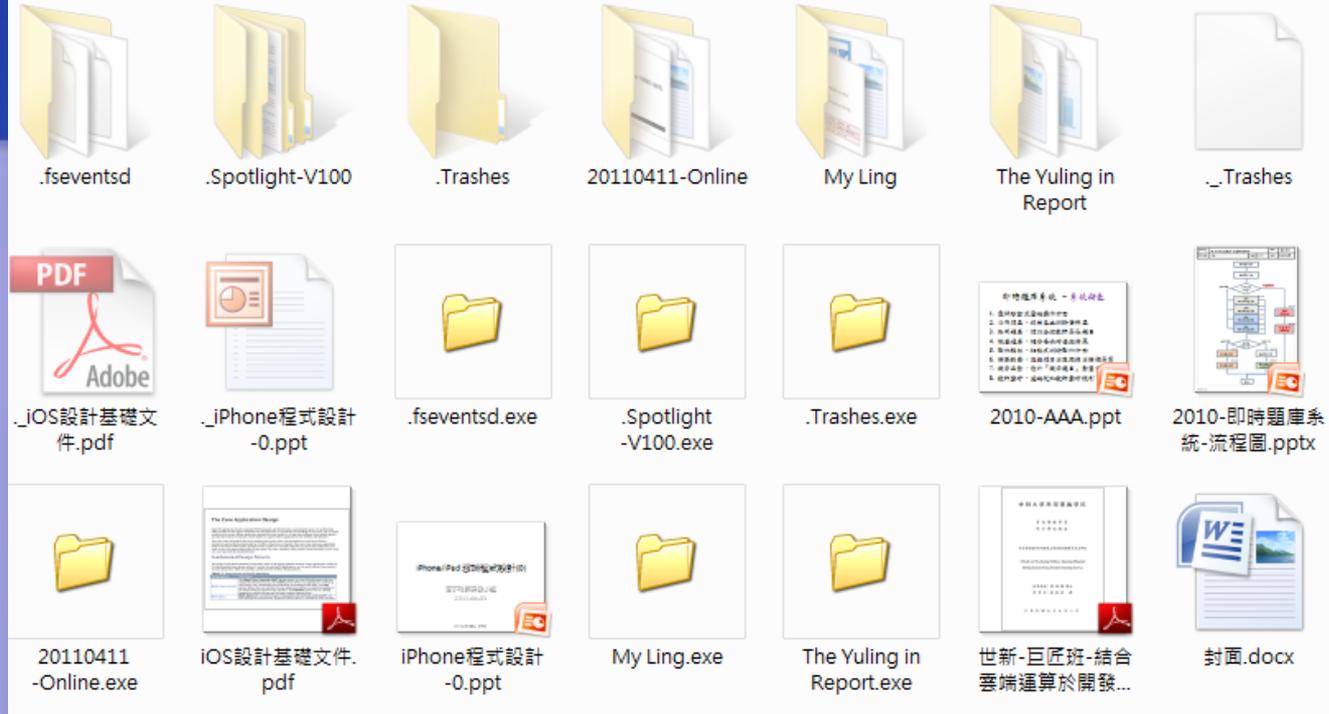
- 桌面
- dmliu
- 公用
- 電腦
- VistaOS (C:)
- DATA (D:)
- DVD RW 磁碟機 (E:)
- USB (F:)
- BD-ROM 光碟機 (H:)
- 網路
- 控制台
- 資源回收筒
- GodMode.{ED7BA470-8E54-465E-825C-99712C}

名稱 修改日期 類型 大小 標記



名稱 修改日期 類型 大小 標記





# Stuxnet - 歷史新發展

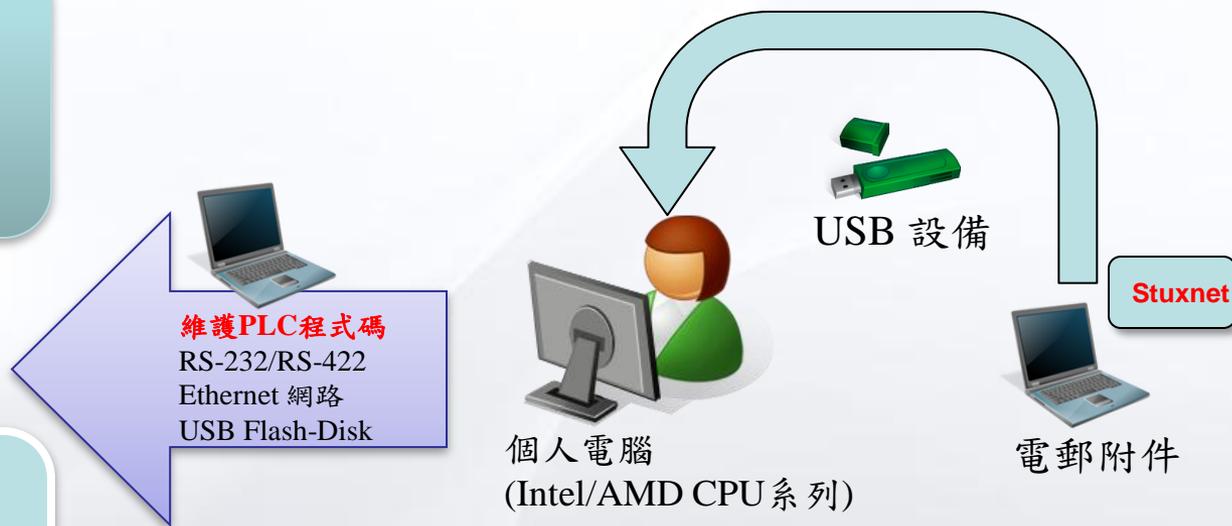
- 2010-06，歷史上，第一個從個人電腦感染工業(醫療)控制器的跨系統(攻擊型)電腦病毒，相當於生物界的『異種』感染病毒。

工業設備  
(非電腦)

已感染 PLC  
(西門子 siemens 系列)

工業設備  
(非電腦)

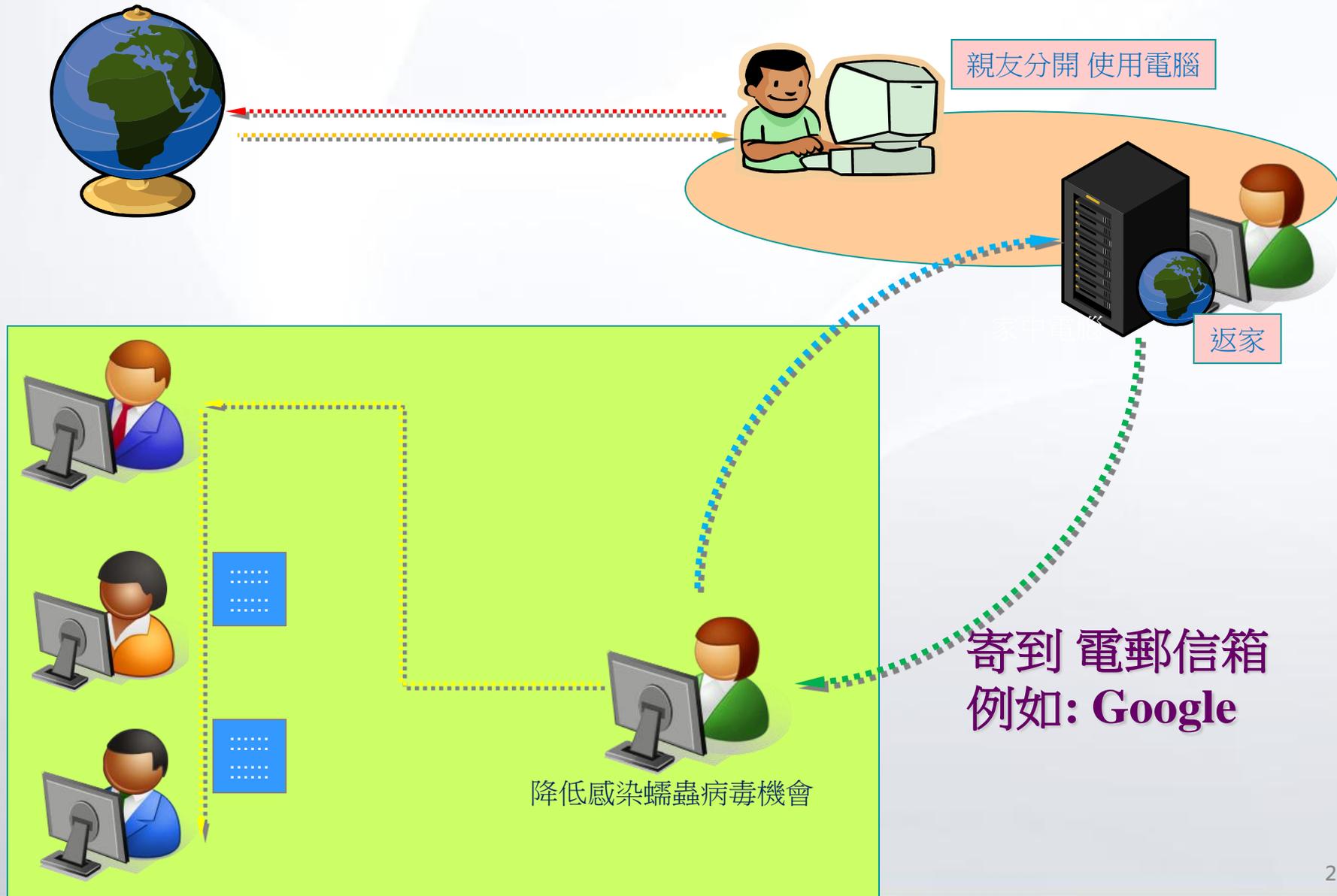
未感染 PLC  
(GE, 西屋, HP 等等系列)



NSS researcher Dillon Beresford reported finding "multiple vulnerabilities" in Siemens programmable logic controllers (PLCs) used in plants worldwide to automatically regulate temperatures, pressures, turbine speeds, robot arms and more.

"This is a global problem," NSS chief executive Rick Moy told AFP.  
"There are no fixes to this right now," he continued "Bad guys would be able to cause real environmental and physical problems and possibly loss of life."

# 私人電腦 與學校電腦 的隔離措施



分享MOD再享超值優惠 票選人氣『金』好創意 新手安心購屋須知 廣達 要當雲端受惠王

網頁郵件 通訊錄

現在位置：網頁郵件 > 讀信

# 讀取信件

WEBMAIL @ HINET 登出

→ 搬移至...

回信 全部回信 轉寄 檢視信件原始檔 友善列印 下載信件 刪除

dmliu: 收件匣

上一封 | 下一封 | 返回 | 另開視窗閱讀信件

寄件人：何 < honhungmen@yahoo.com.tw > 加入通訊錄 檢舉垃圾信

收信人：aglowdзи@gmail.com

日期：Thu, 2 Jun 2011 15:23:22 +0800 (CST)

主旨：麥當勞疑似廣告不實

附檔：我自己拍ㄉ相片.rar(89.7K)

[字體] [語系]

副檔密碼是123哦^^

檔案下載

是否要開啟或儲存這個檔案?



名稱：我自己拍ㄉ相片.rar

類型：WinRAR 壓縮檔

從：sg1000.webmail.hinet.net

開啟舊檔(O)

儲存(S)

取消



雖然來自網際網路的檔案可能是有用的，但是某些檔案有可能會傷害您的電腦。如果您不信任其來源，請不要開啟或儲存這個檔案。[有什麼樣的風險?](#)

您的交易網站安全嗎?

寫新信

信件匣 [管理]

收件匣 >>

草稿匣

寄件備份

歷史信件匣

垃圾桶 [清空]

垃圾信件匣 [清空]

我的信件匣

我的同事

我的同學

我的家人

我的朋友

真理大學

外部信箱

玲欢蔓藤踏戀 珍 戀戀  
狹 十 暑 30じど 狹都  
盾???







(線上)

Chinese (中文)

免费的表情图释和传情动漫！

# Bando



下载

许许多多好玩的表情图释和令人目眩的动态传情动漫给您的朋友带去惊喜！  
完全免费！Bando支持QQ、Windows Live Messenger (MSN)、Hotmail、Facebook、Gmail、Yahoo IM和Mail以及Outlook Express等聊天和电子邮件程序。



点击这里！  
免费下载！

没有间谍软件/没有广告软件/没有特洛伊木马病毒/没有弹出窗口

[点击这里下载Bando!](#)

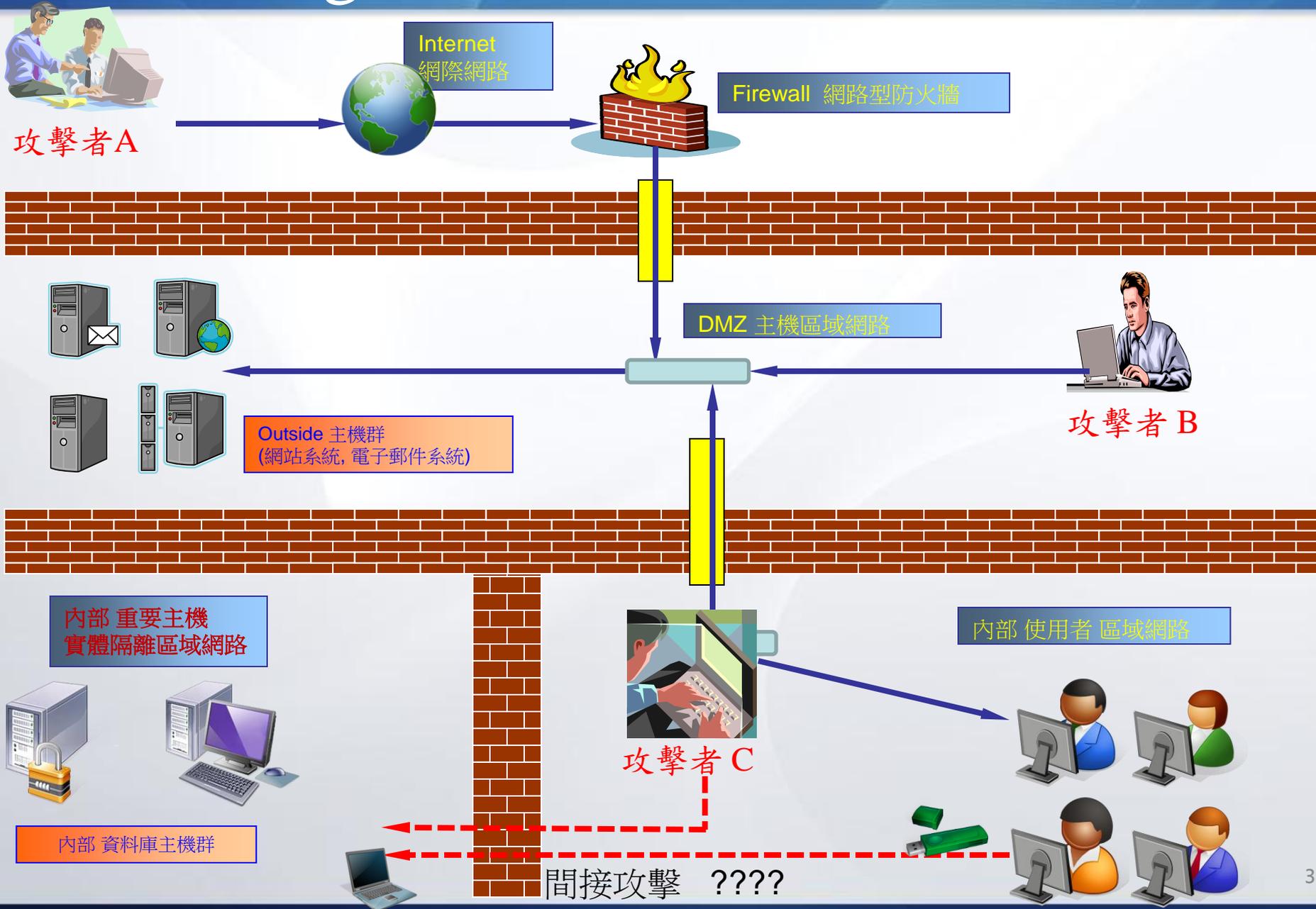


下载Bando并获得好玩的免费表情图释、传情动漫和闪屏振动！

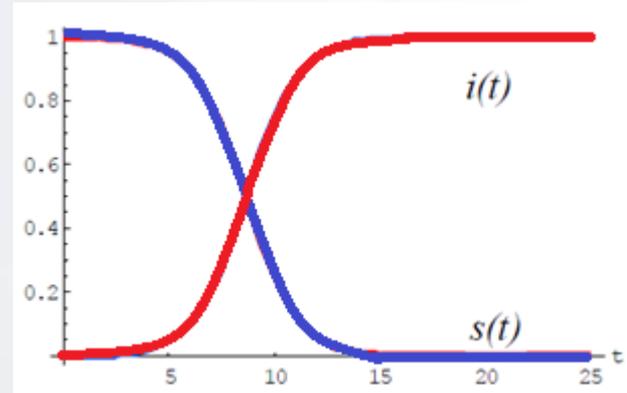
Bando给您好玩的新的方式在QQ, Live Messenger, Hotmail, Yahoo IM & Mail, Facebook, Gmail 以及 Outlook Express中表达您自己，给您的对话送去无尽的乐趣和惊喜！



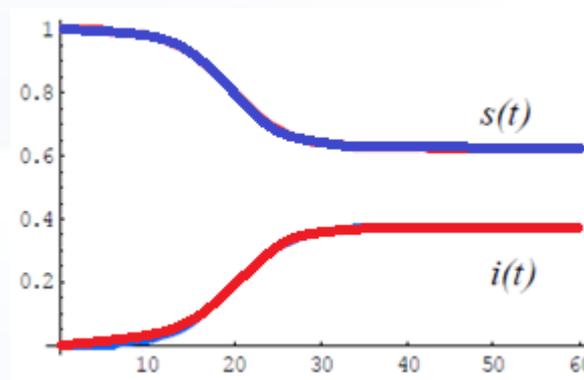
# Diagnostic Tests on Network



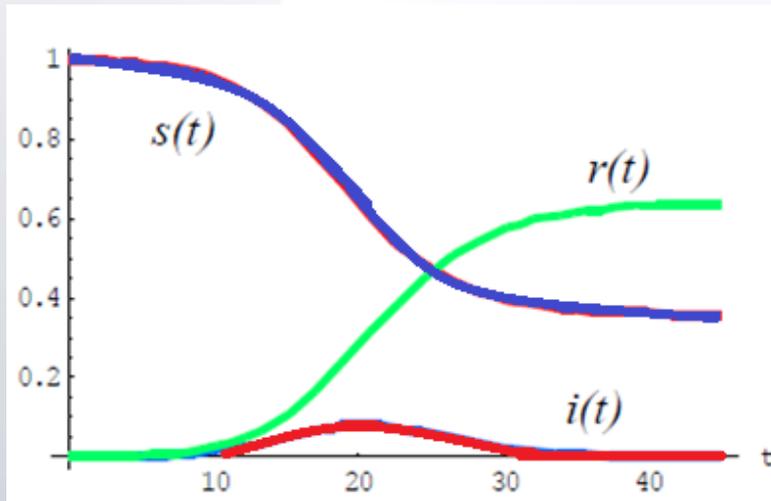
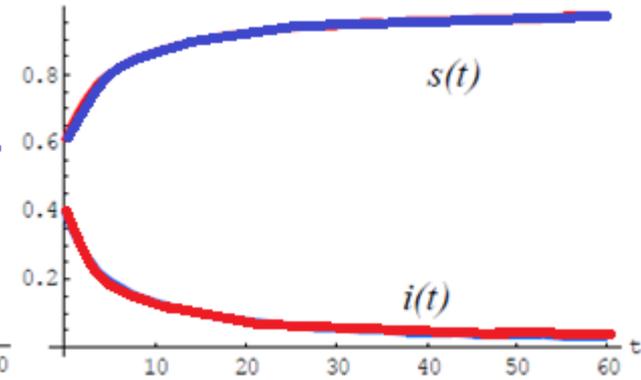
# Diagnostic Tests and Forensics



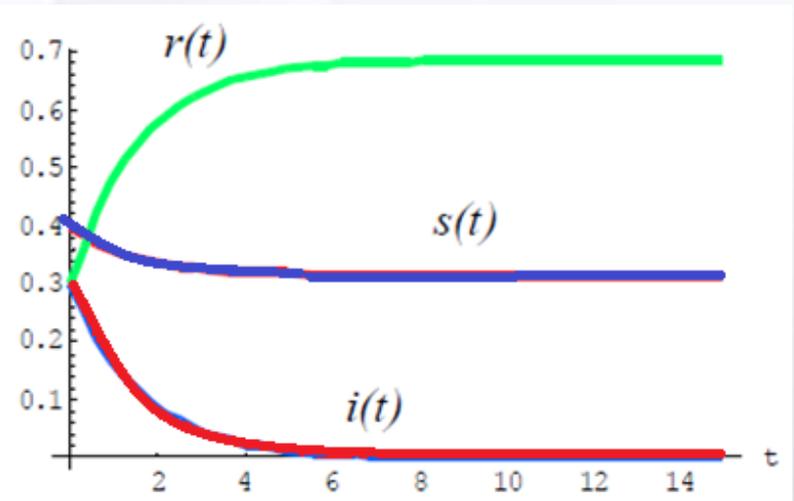
SI 模型  
(無病毒碼的防毒系統)



SIS 模型  
(中毒後，電腦重新安裝)



SIR 模型  
(有病毒碼的防毒系統)



# 雲端技術的簡介

- 上層分級: 雲端軟體 Software as a Service (SaaS)
- 中層分級: 雲端平台 Platform as a Service (Paas)
- 下層分級: 雲端硬體 Infrastructure as a Service (IaaS)
- 使用者專注於自身應用需求，而無需擔憂系統相容與品牌

有線網路、無線網路、主機硬體



MS-Windows、Linux、SQL、Web

資料查詢、訊息發佈  
模擬計算、影音處理



# 雲端運算的資料安全探討

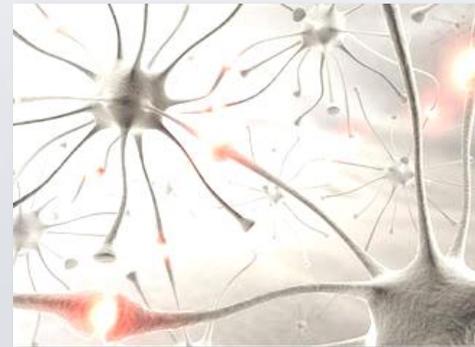
- 資安三目標 資料、資產、隱私 沒有改變。
- 資安三威脅 也跟隨到雲端 變得更複雜。
- IaaS, PaaS, SaaS 的重要核心技術之一
- Virtualize (虛擬化) 正遭受駭客努力研究
  - 虛擬機器 Virtual Machine 是否是安全環境?
- Joanna 的 Blue-Pill與Red-Pill

"The Red Pill" –2007 BlackHat  
Joanna Rutkowska

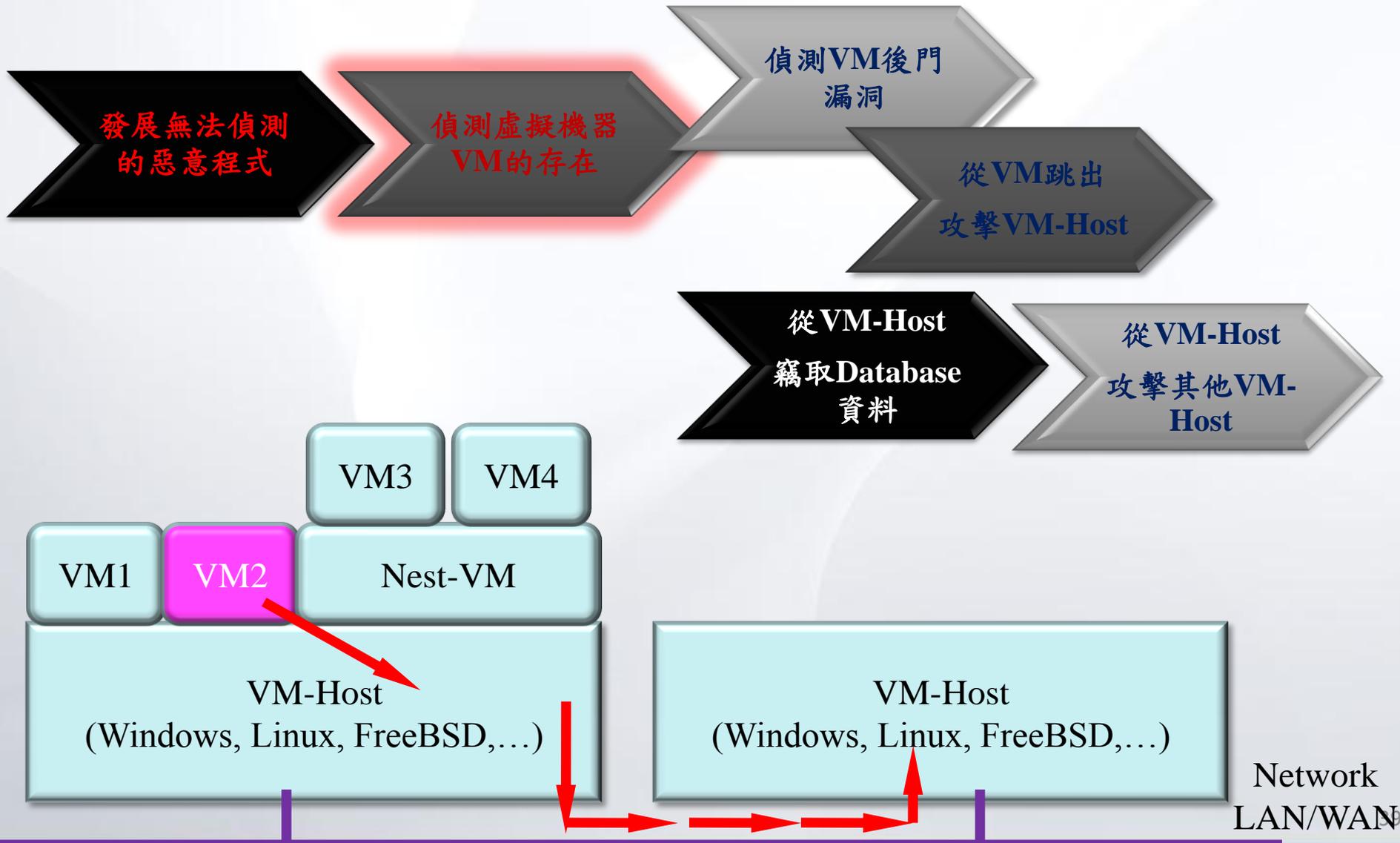


# 雲端運算的資料安全探討

- 資安三目標 資料、資產、隱私 沒有改變。
- 資安三威脅 也跟隨到雲端 變得更複雜。
- IaaS，PaaS，SaaS 的重要核心技術之一
- Virtualize（虛擬化）正遭受駭客努力研究
  - 虛擬機器 Virtual Machine 是否是安全環境？
  - 2006-Blue Pill, Creating undetectable malware on x64 ...
  - 2007-SubVirt: Implementing malware with virtual machines
  - 2007-Attacks on Virtual Machine Emulators
  - 2008-Red Pill, Detecting Virtual Machine ...
  - 2010? 2011? 2012 ? ...



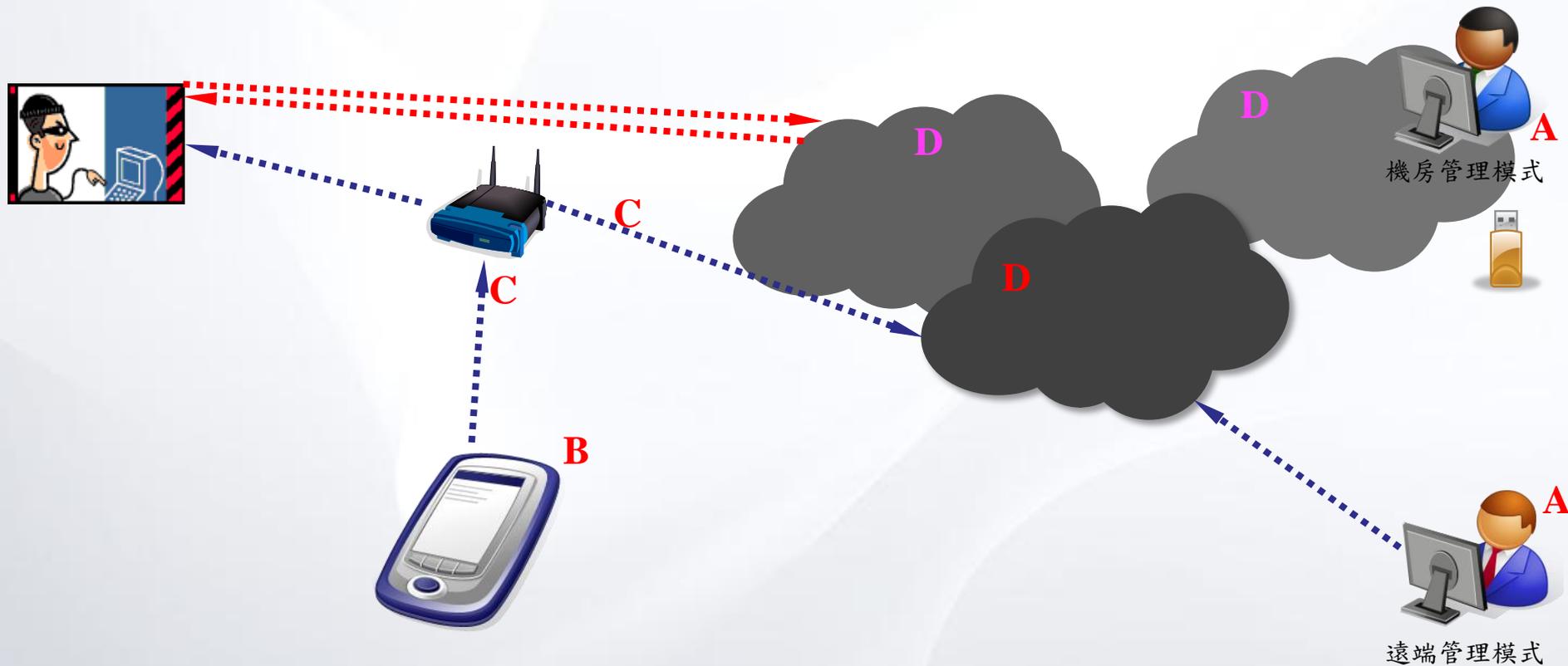
# 雲端系統的資料安全



# 主機外包廠商會不會有問題？

- 高科技網路維護公司的工程師的特質
  - 具備網路知識與主機重要訊息(帳號, 密碼, 檔案)
  - 個人背景因素, 不易查證(就業時無須查證有無前科紀錄)
  - 案例1: 奇美電子工程師曾經撰寫木馬程式並且在網路販售, 史稱『網路徵信社案件』。
  - 案例2: 新竹某國立大學, 研究所學生自製木馬程式販售, 並且偷窺被害人電腦資料, , 史稱『大鳥木馬案件』。
- 有無記錄進出機房的整體過程?  
(攝影機, 記錄簿, 服務記錄單)
- 有無記錄維護主機的整體過程?  
(帳號, 影像, 操作畫面)

# 雲端運算的資料安全探討



## 駭客可能攻擊模式

- A. 雲端系統管理員 (Administrator) 例: 社交工程, 惡意程式, 後臺入侵
- B. 用戶端行動設備 (Browser) 例: 惡意程式(PDF), 自身漏洞
- C. 雲端系統中繼網路 (Connection) 例: Wireless-Sniffing, DNS-Spoofing
- D. 雲端系統自身系統 (Database) 例: VM惡意程式,X-Injection

# Google有多安全?!

## 信用卡中心有多安全?!

- 多數雲端技術供應商，其過去產品的資安紀錄，耐人尋味!! Cisco如何? Microsoft如何? Oracle如何?
- 廠商的產品資安記錄，就如同歷史教訓一樣，會不會重演各種感染病毒蠕蟲與產品漏洞的歷史劇碼呢?
- 一般網管人員最認為安全的Google有多安全呢? 資訊安全歷史教訓告訴我們，Google的平台最不易被駭客入侵，但是在2010年3月份，中國大陸的Google公司內部被竊取的是系統加密的公鑰，然後所有重要異議人士的GMAIL電郵信箱內容，逐一被竊!!
- 與其相信某家廠商的產品資安技術，不如假設該資安技術已經被駭客破解，那雲端資料庫內容能否抵擋駭客竊密解譯?

# 網路安全的基本防護方式

- 不自行下載軟體程式 (政府網站除外)
  - 如果要下載程式，請至官方網站(Official Web)。
  - 不要相信任何入口網站的下載檔案或程式。
- 不要互相傳送電子郵件的可愛檔案
  - 不要自行安裝私帶的程式。(包括免費軟體, 螢幕保護程式)
  - 不要安裝**破解版**的電腦程式或防毒軟體。
  - 不要執行(開啟)電子郵件的危險附件檔案(exe, pif, com, scr, ...)。
- 請隨時更新(**請勿關閉**)電腦漏洞補強機制
  - Windows Update 漏洞自動修補機制
  - 防毒系統病毒碼更新機制
  - PDF Viewer 最新更新程式
- USB設備(拇指碟)已經成為病毒溫床，請不要帶USB資料回家。
- **駭客會採用最熟悉的方式欺騙被害人**。包括有：熟悉的朋友電郵帳號、常用的同事電郵帳號、最近的會議活動名稱等等，其中的電郵附件檔案就是病毒木馬的檔案。

# 網路安全的 資安五要

- 網路視訊有漏洞，平常要關閉
  - 木馬後門會進行『視訊偷拍』
  - 不用WebCam視訊的時候，要將它『停用』。
- 網路照片要謹慎保管好，不要交給別人保管
  - 許多知名部落格都有漏洞，私密照片不要上傳。
  - 現任男友，也許會成為『歷史遺跡』，私密照片要加密。
  - **X 不要自拍裸照、不要用電腦做「害羞的事」...**
  - **X 如果男友要求你跟他自拍害羞的照片，休掉他！**
- 電腦送修前要先備份重要資料，並刪除私密檔案
  - 不要讓維修廠商複製電腦檔案的機會。
  - 現任男友，如果是電腦高手，他也可能會幫你安裝木馬後門
  - (安裝木馬後門只要5秒鐘，就可以監控msn,開啟WebCam)
- 網路交友要謹慎，社群網站是最好的偽裝機制
- 要經常參加各類資安研討會

# Q&A

- Name : Diamond Liu (a.k.a Jamien Liu)
- Email : [dmliu@ms4.hinet.net](mailto:dmliu@ms4.hinet.net)
- MSN : [dmliu99999@hotmail.com](mailto:dmliu99999@hotmail.com)
- Address: Diamond InfoTech.
- Taipei, Taiwan, R.O.C.

My first wish is to see this plague of mankind, war, banished from the earth.

George Washington, 1st US President