蔡一郎

從台菲衝突看網路攻擊技術之發展趨勢

大綱

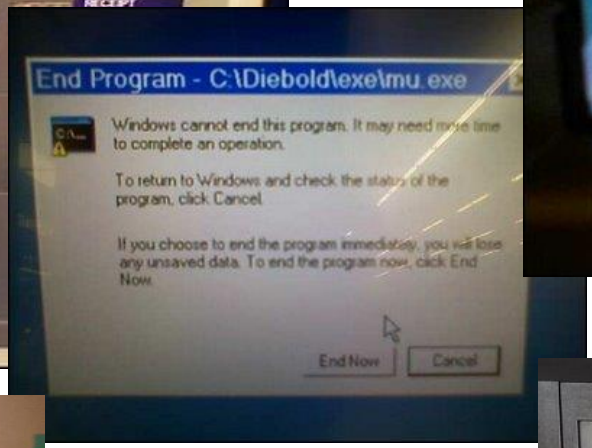
- 從我們的生活環境談起
- 駭客行動主義盛行
- 從駭客思維看資訊安全問題
- 台菲網路攻擊事件
- 殭屍網路的威脅

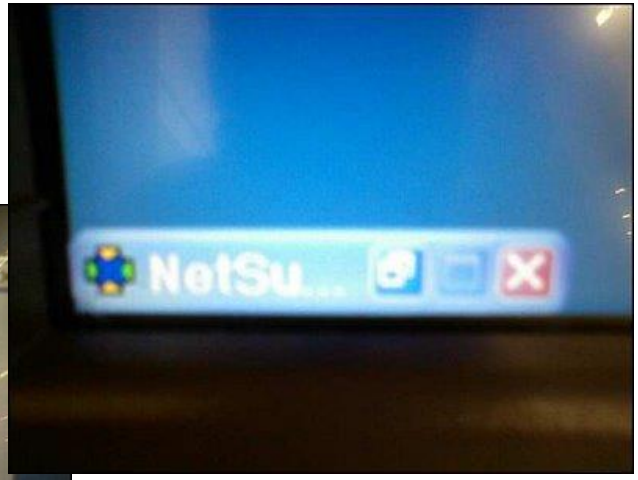
您有發現隱藏的問題？

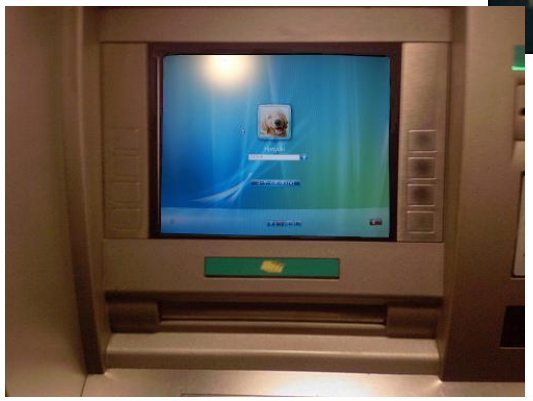
NARLabs

承諾·熱情·創新

- 當ATM使用windows時…







續集...

- 其它ATM的問題...

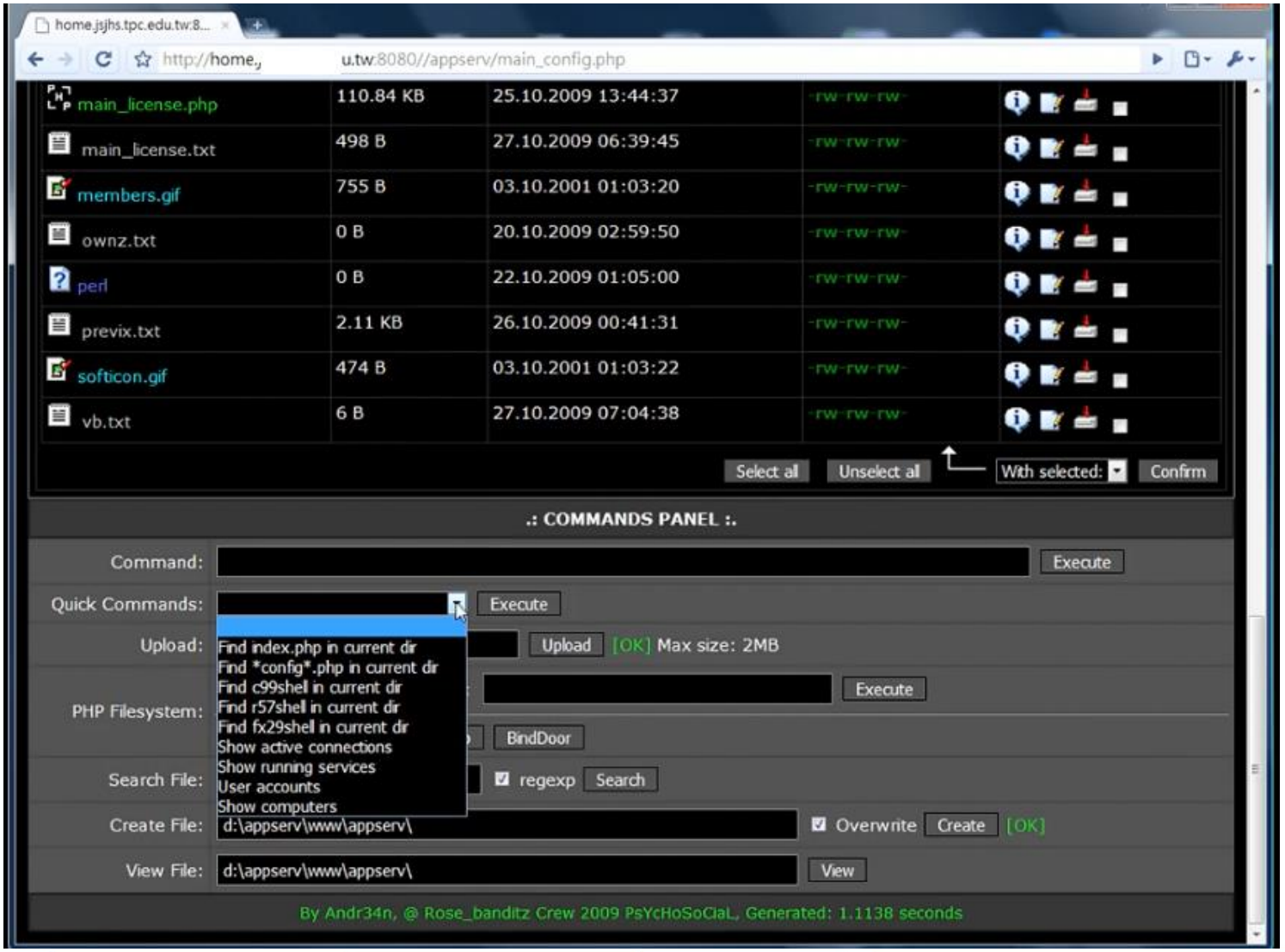
Blackhat 2010…

- 日常生活的資訊系統
- 原本被認為是安全的設備
- Blackhat 2010 現場展示如何控制ATM

中繼站的後台...

NARLabs

承諾·熱情·創新

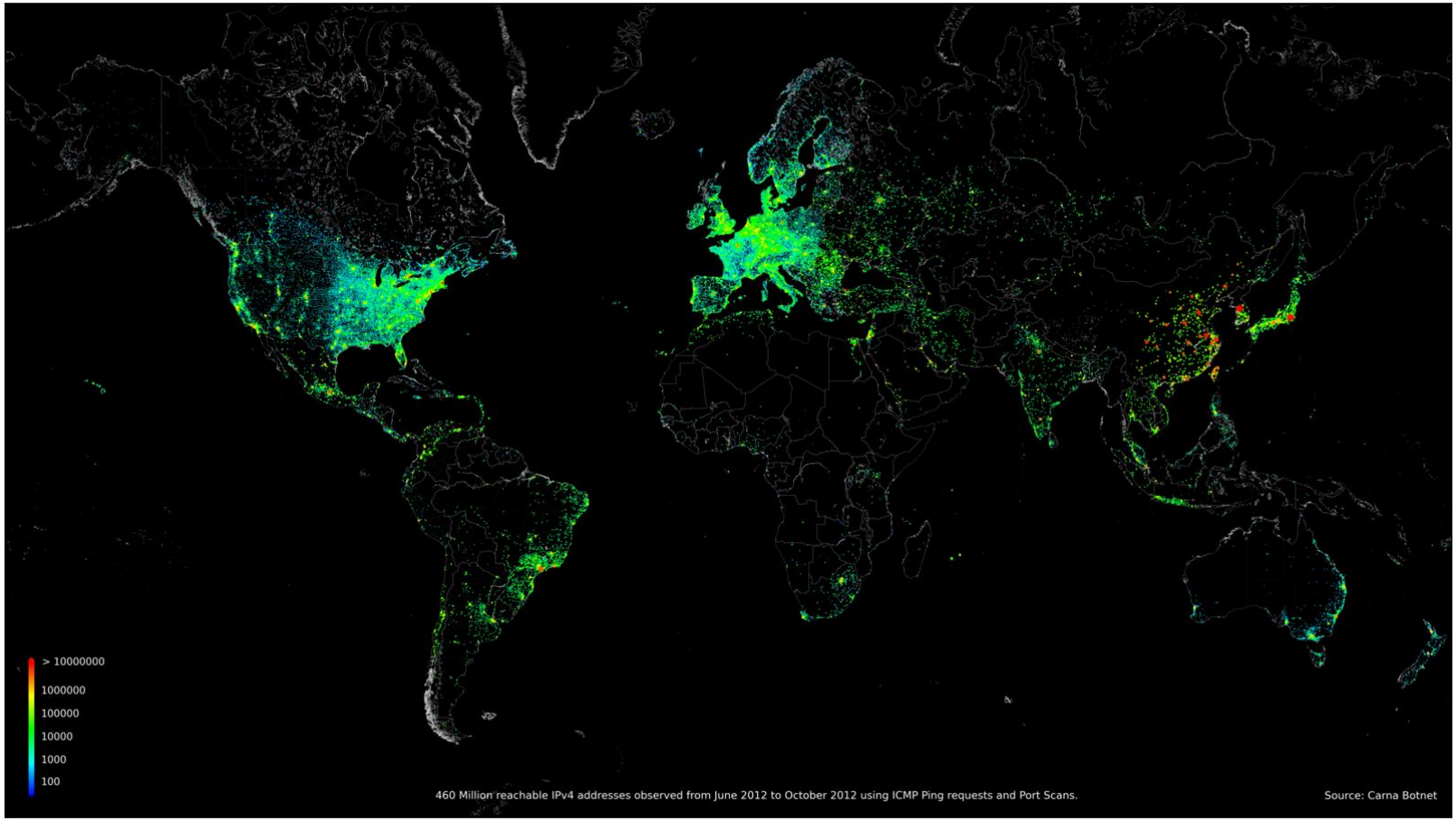


APT的範圍...

NARLabs

承諾·熱情·創新

- Public: 全世界460,000,000 IPv4位址...
- Private: 不計其數...



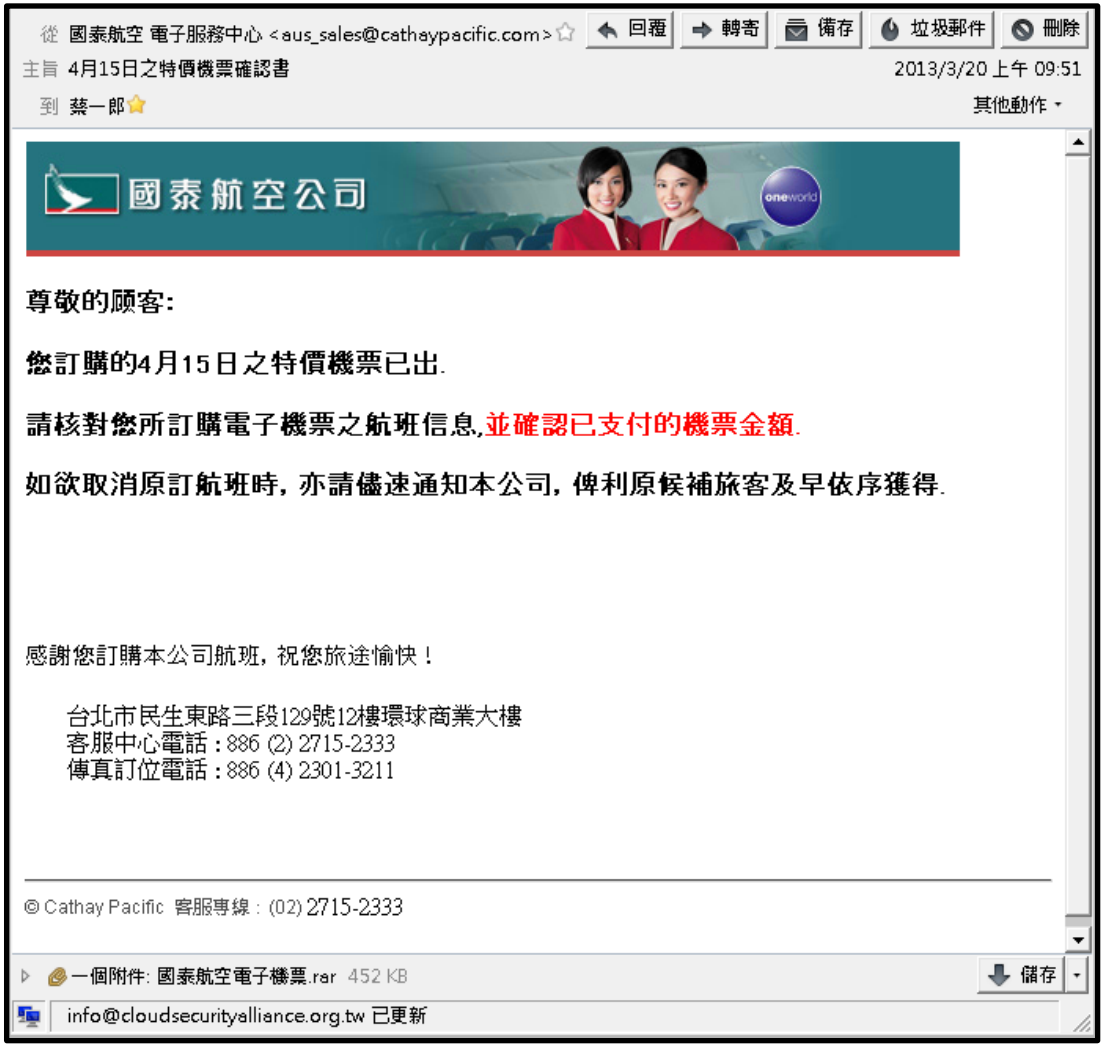
資料來源： http://internetcensus2012.bitbucket.org/paper.html

APT的管道？

NARLabs

承諾·熱情·創新

- 電子郵件
- 線上傳訊
- 社群網路
- 掛碼網站
- 社交工程
- …



最近的事件...

NARLabs

承諾・熱情・創新

資安公司：南韓網路癱瘓事件手法不同以往 以破壞摧毀為目的

鉅亨網新聞中心　2013-03-22 10:19:11　Blog談新聞 評論(0) 下則

南韓在本月 20 日發生主要電視台及多家銀行電腦被駭事件，據網路攻擊防護廠商FireEye®公司表示，不同於過去事件，這次惡意軟體攻擊南韓的重心在癱瘓、摧毀被攻擊的系統，而非竊取資料。

FireEye 研究部門總監 Rob Rachwald 指出，過去，駭客採用分散式阻斷服務 (DDoS) 的手法，攻佔一個國家的基礎設施，2007 年對愛沙尼亞的網路攻擊，2012 年宣稱由伊朗駭客軍團對美國數十家銀行發動的攻擊等，均屬此類。

Rachwald 說，這次針對南韓的攻擊，重點是損毀主開機紀錄 (MBR)，抹除硬碟所有資料，並造成電腦當機。同時，此一惡意軟體有定時功能，也就是軟體原本在睡眠狀態中，但設定在特定時間啟動－南韓時間 3 月 20 日下午 2 點

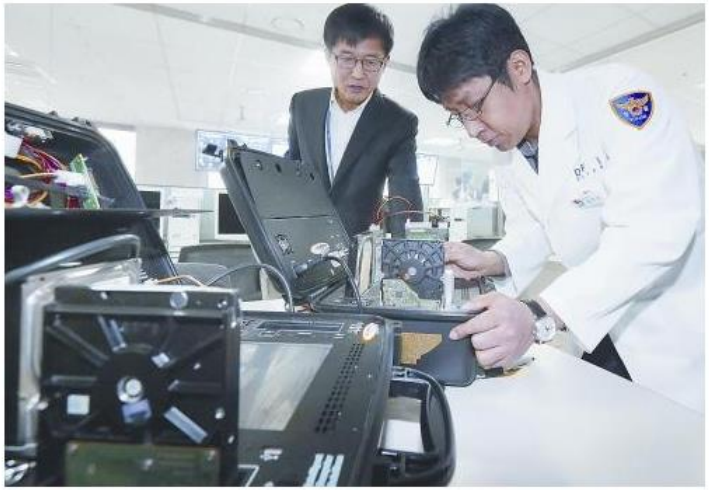
啟動後該惡意軟體即檢查 Windows 版本，發動一個執行緒，再直接寫入硬碟中，進而毀掉主開機紀錄。最後，此軟體具備回避功能，它會檢查並停用韓國流行的防毒產品 — AhnLabs。FireEye 公司強調，這說明駭客擺明是衝著南韓而來。

FireEye 指出，他們抵擋了這次攻擊，並偵測、命名此惡意軟體攻擊為 Trojan.Hastati。FireEye 說，這個惡意軟體不會進行 CnC 回撥 (callback)，完全以破壞中毒主機為目標。它清點 Microsoft Vista 及其後續版本 (Windows 7 / 8) 系統上的所有檔案，將關鍵字「HASTATI」覆寫到所有檔案上，接著刪除被覆寫的檔案，使資料無法復原。而對較早期的 Windows 版本，該惡意軟體會覆寫邏輯磁碟，在損毀/覆寫主開機紀錄後將系統重新開機，進而癱瘓系統。

根據南韓所做調查，發現惡意代碼來自中國，並相信是北韓所做。《韓聯社》報導，政府相關人士表示，由於南韓基礎建設控制系統採封閉式網路，因此北韓鎖定相關合作企業的電腦進行攻擊，並預期未來還會針對交通、電力及金融網路的薄弱環結，進行多方面攻擊。

南韓公佈網路攻擊調查結果 疑平壤駭客幕後操縱

2013-03-22 05:53:41 | 來源：環球時報 | 編輯：李喆 | 發表評論 進入論壇>>



21日，在南韓首都首爾，網路安全人員正在檢查南韓廣播公司受到網路攻擊的硬體設備。

【環球時報綜合報道】究竟是誰對南韓的銀行和電視臺發動了大規模網路攻擊，導致3萬多臺電腦癱瘓？南韓跨部門調查小組昨天給出初步答案：攻擊的一個IP地址源頭來自中國。不過，南韓官方以及國際媒體沒人懷疑是中國發動的攻擊，朝鮮被公認是“最大的嫌疑人”，據稱朝鮮駭客經常利用中國的電腦攻擊美韓。

朝鮮昨天對此沒有直接回應。當天，朝鮮拉響防空警報，朝鮮人民軍最高司令部發言人警告說，要對包括沖繩、關島在內的美軍太平洋軍事基地發動核打擊。朝鮮官方媒體刊登多篇文章強烈抨擊美軍將具備核打擊能力的B-52轟炸機高調引入朝鮮半島，認為這是為侵略朝鮮做準備，“美帝在越南戰爭、海灣戰爭、阿富汗戰爭時都曾投入這種戰略轟炸機”。

21日，美韓“關鍵決斷”軍演結束，但朝鮮半島的緊張和敵意仍在攀升。此前美韓許多分析家認為，朝鮮會在軍演之後“做出挑釁”。韓軍發言人稱，將繼續對平壤保持高度警戒，因為“很難預測朝鮮飛機什麼時候、在哪發動攻擊”。

續集...

NARLabs

承諾・熱情・創新

3月20日韓國史上最大駭客攻擊事件調查出爐，北韓至少策畫了8個月來主導這次攻擊，成功潛入韓國金融機構1千5百次來部署攻擊程式，受駭電腦總數達4萬8千臺

韓國於4月10日發表320駭客攻擊事件的期中調查報告指出，發動攻擊的首腦是北韓。

照片來源：韓國MSIP

韓國在3月20日遭遇了史上最大規模的駭客攻擊行動後，韓國政府、軍方及民間資安廠商合組成民官軍聯合應變小組展開調查，並於4月10日發表了期中調查報告，策動攻擊的首腦正是北韓。

韓國官方在報告中指出，此次攻擊事件為北韓主導，駭客攻擊所使用的IP(175.45.178.XX)，註冊地址為平壤柳京洞，受駭的電腦、伺服器與ATM伺服器數量，也比韓國資訊安全局（KISA）3月底時公布的3萬2千臺更多，最後統計有4萬8千臺設備遭駭故障。

而且此次攻擊至少歷經8個月的精心策畫，來搜集目標企業內部電腦與伺服器的相關弱點，駭客不斷嘗試任何可以入侵的漏洞，至少有6臺北韓電腦從去年6月28日開始，成功潛入這些受害金融機構約1,590次來上傳惡意程式，駭客因此而掌握了這些企業的資訊系統弱點與防範鬆懈的部份，才能夠一次就造成如此大規模的設備癱瘓。

民官軍聯合小組的技術人員發現，這次攻擊路徑涉及韓國25個地點、海外24個地點，部分地點與北韓之前發動網路攻擊所使用的地址相同。而且，駭客所植入的惡意程式總共有76種，其中9種具有破壞性，其餘惡意程式僅負責監視與入侵之用。文⊙張景皓

Thinking…

如果…
發生在台灣呢？

其實只要這樣就行了…

是方電訊大樓機房失火釀全臺網路大當機，10年來最慘烈網路災難

文/曾筱媛 (記者) 2013-03-04

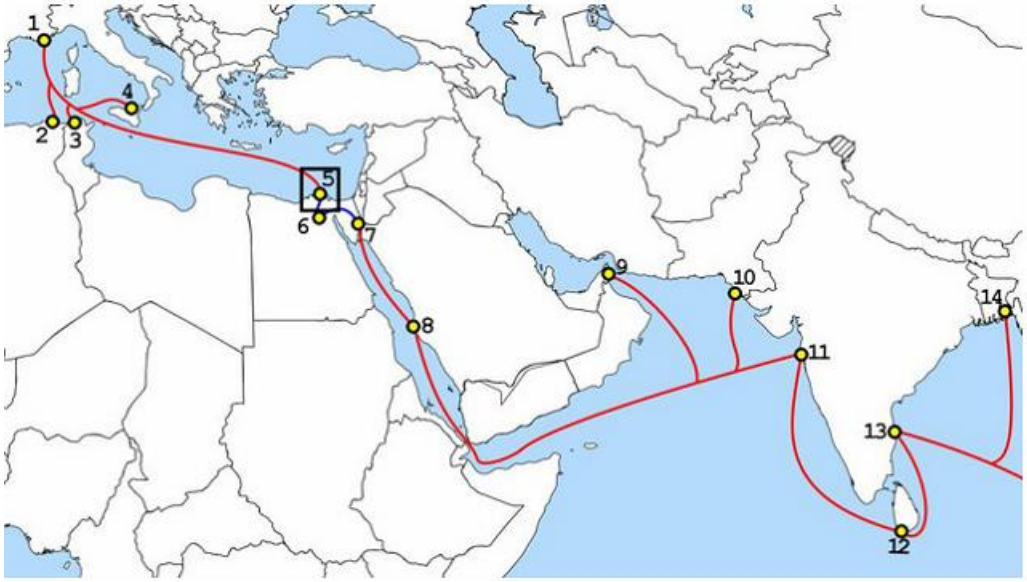
讚 37　Share　+1 6　我要收藏

位在臺北市內湖區的是方電訊總部大樓發生火警，造成全臺網路癱瘓，甚至包括臺灣多數ISP業者的對外海纜都出問題，Yahoo、台灣高鐵、微軟MSN、中華電信、遠傳、台灣大寬頻、威寶電信等都坦承受影響

2月25日位於臺北市內湖區陽光街巷弄內的麗源大樓發生火警，是方電訊、數位通國際（eASPNet）2家機房服務停擺。

元宵節剛過，臺灣就意外頻傳。全臺網路交換重鎮的是方電訊總部大樓（麗源大樓），在2月25日上午發生火災，大樓供電因消防滅火安全而斷電，導致全臺9成對外海纜網路服務，以及諸多網站、網路服務被迫中斷12個小時以上。災情波及臺灣多數的ISP業者，許多知名網站也因此停止服務，民眾更明顯感受到網路連線異常變慢，甚至連3G網路也受到影響。

又有續集...



被捕的地點位於埃及海底電纜的中央位置，電纜屬於埃及電信公司所有，而這個節點往東連接開曼、沙烏地阿拉伯等中東國家，往西連接義大利、摩洛哥、突尼西亞、利比亞等國家。如果這個節點一旦中斷，東方與西方之間的網路將會大受影響。

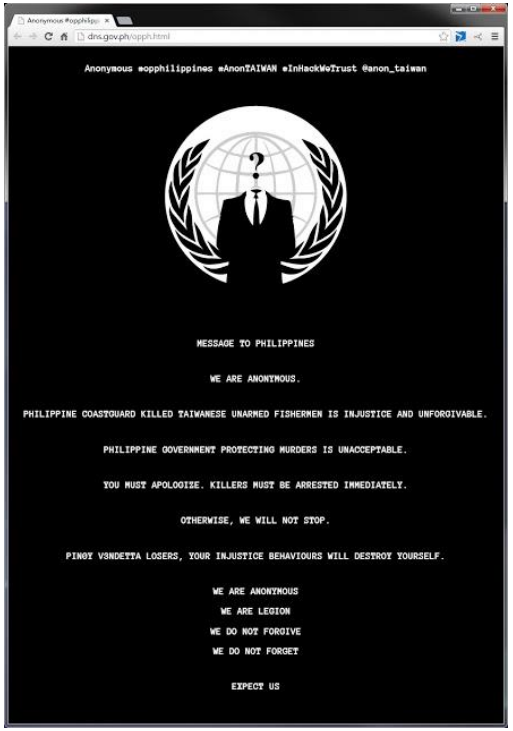
三個埃及潛水夫用行動告訴我們，他們根本不需知道什麼是 DDoS 技術，只要有一把刀跟潛水工具，就能影響網路世界！

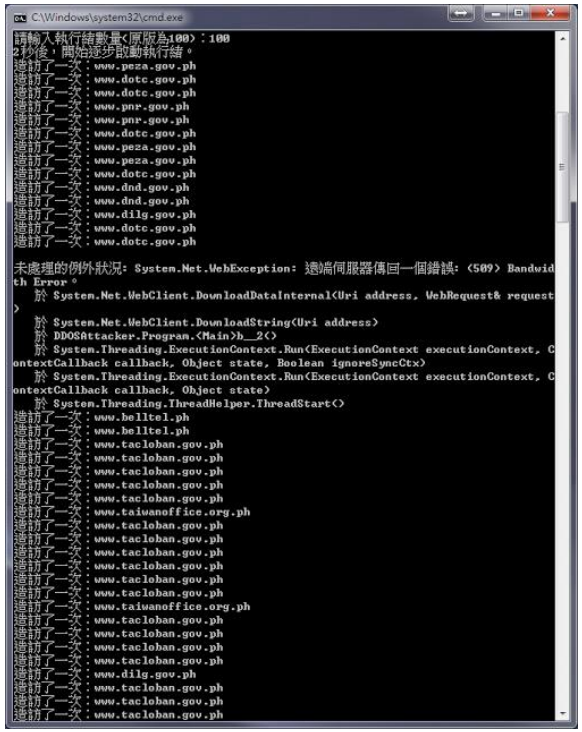
談台菲網路攻擊事件

NARLabs

承諾·熱情·創新

- 因真實世界的國際問題而引起
- 真實世界仍在處理程序問題時，虛擬世界早就戰火遍野





台菲網路攻擊的技術分析

NARLabs

承諾·熱情·創新

- DDoS分散式阻斷服務攻擊
  - 進行高頻率的網頁更新要求
    - 網頁版、手機版
  - 利用DDoS工具進行特定目標攻擊
- SQL Injection資料隱碼植入攻擊
  - 網站未檢查使用者輸入字串
  - 配合Google Hacking搜尋對象
  - 使用網站爬蟲程式進行網站結構分析
- 系統與應用程式漏洞
  - 古老的問題，但是最有效
  - 配合Malicious Exploit Code

台菲網路攻擊的技術分析

NARLabs

承諾·熱情·創新

- 一攻一防之間，運用匿蹤的技術
  - 開放服務的Proxy
  - 網路上的隱匿服務
    - SafeIP

防禦相關技術

NARLabs
承諾·熱情·創新

- DDoS分散式阻斷服務攻擊
  - 偵測到DDoS攻擊行為，則必須完成再次認證
  - 依賴流量過濾業者提供「清洗」服務
  - 加大網路頻寬、系統資源
  - 縮小應用服務Timeout時間設定
- SQL Injection資料隱碼植入攻擊
  - 加入字串檢查機制
  - 重新檢視網站程式
- 系統與應用程式漏洞
  - 修補已知系統與應用程式漏洞
  - 配合資安設備進行防禦

社群網路的時代

NARLabs

承諾·熱情·創新

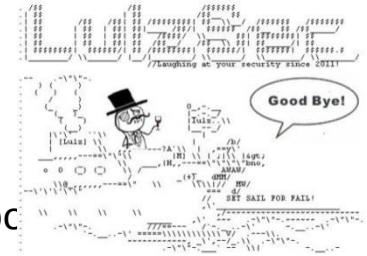
- 實名制?
- 台灣流行的BBS
  - 台大PTT、巴哈姆特、台大椰林風情、政大貓空行館、東海大度山之戀
- SNS
  - Social Network Service
  - Social Network Software
  - Social Network Site
- 建立人際網路

人人網

Facebook

駭客行動主義(Hacktivism)的威脅

- 自2011年起大規模的網路攻擊行為激增，並且造成實質影響
- 營運規模越大、擔任的角色越重要，將越容易成為主要攻擊目標
- 目的
  - 意圖破壞或癱瘓某個組織的服務、竊取使用者的資料，或在攻擊後在網站上留下訊息，以針對訴求的意見，引起關注或表達抗議
- 手法
  - 結合多種攻擊技術(Malware、Botnet、APT)與環境(Web-Based、Cloud Services)，進行大規模針對性攻擊
- 對象
  - 政府單位、組織
  - Amazon、Sony、Google、RSA、Facebook、Dropbo



資訊安全問題

NARLabs

承諾·熱情·創新

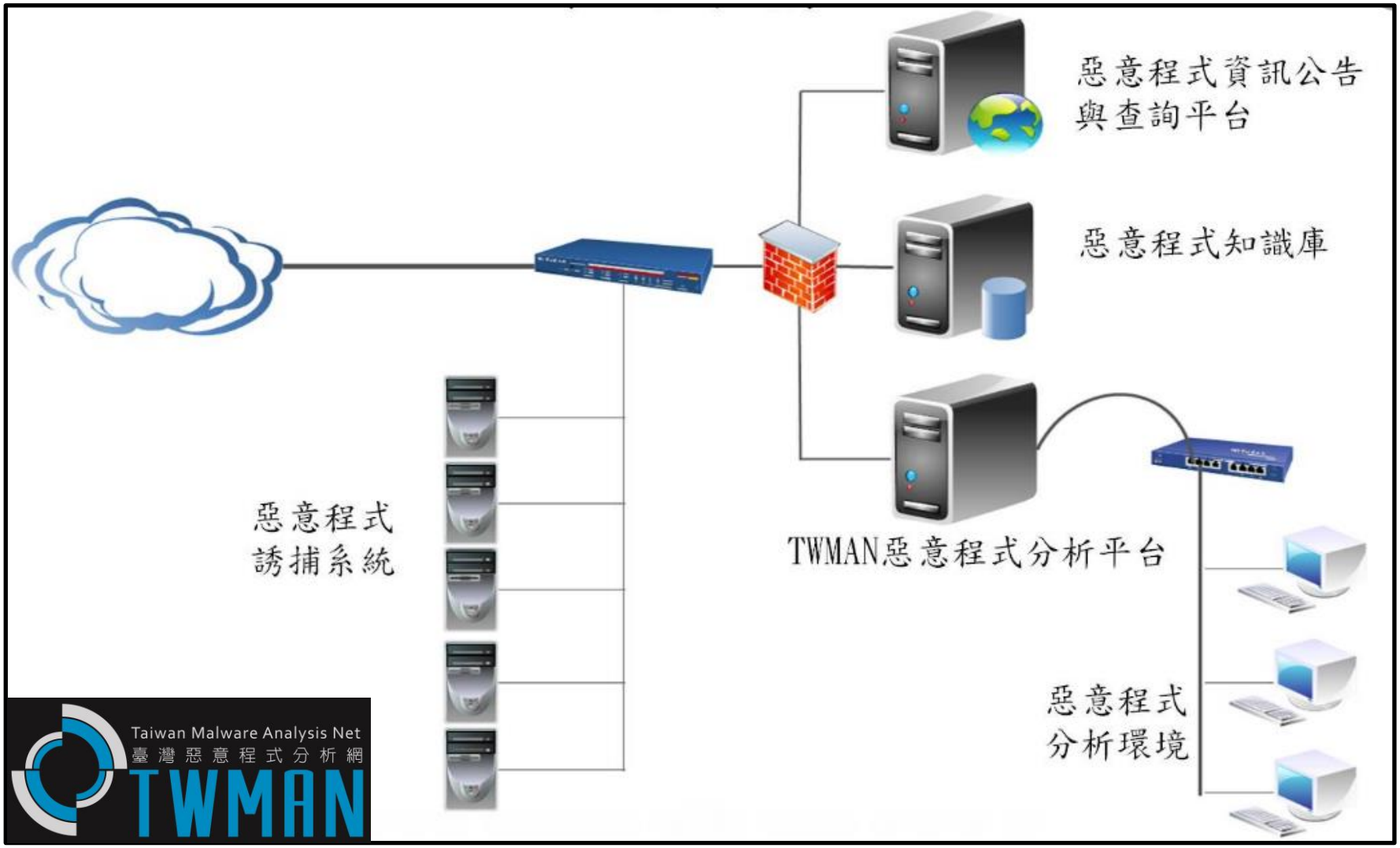
- 從事件調查看資安問題
- 新型態的攻擊層出不窮
- 傳統安全防禦機制失靈
- 複雜且難以管理的安全政策
- 惡意程式大量出現，自動化攻擊模式影響範圍廣
- 須同時兼顧系統、網路、應用程式與架構上的安全設計
- 身份認證機制
- 無線通訊的安全問題

Security Taxonomy
Mobile Device Security
Encryption
Security Management
Internal Security
Identity & Access Management
Perimeter Security
Storage Security
Physical Security

台灣惡意程式分析網(TWMAN)

NARLabs

承諾·熱情·創新



資安研發平台

NARLabs

承諾·熱情·創新

- 特色
  - 由真實資安事件分析，涵蓋攻擊軌跡與時間戳記
  - 國內Botnet與惡意程式研究平台
- 偵測
  - 由所部署之大量誘捕系統進行多種攻擊行為的掌握
  - 資訊安全設備提供之比對紀錄
  - 網路通訊與流量
- 分析
  - 多樣化Sandbox測試環境(TWMAN、Cuckoo、CWSandbox)
  - 交叉分析(IP、協定、行為等)
  - 資料探勘(Splunk、Hadoop)
- 服務方式
  - 提供線上知識庫查詢服務

Taiwan Malware Analysis Net 臺灣惡意程式分析網 TWMAN cuckoo GFI Sandbox Automated Malware Analysis Tool

惡意程式的入侵(感染)管道

NARLabs
承諾·熱情·創新

- 駭客手法
  - 運用作業系統或應用軟體漏洞植入
- 伴隨Java或active-x程式
  - 結合網頁的設計
- E-MAIL之傳遞
  - 附件、圖片、網頁…
- 即時訊息程式
  - MSN、Yahoo Message、AOL…
- 共享程式
  - Shareware、OpenSource Software
- 瀏覽網頁
- 檔案分享
  - FTP…

現行Botnet的特性

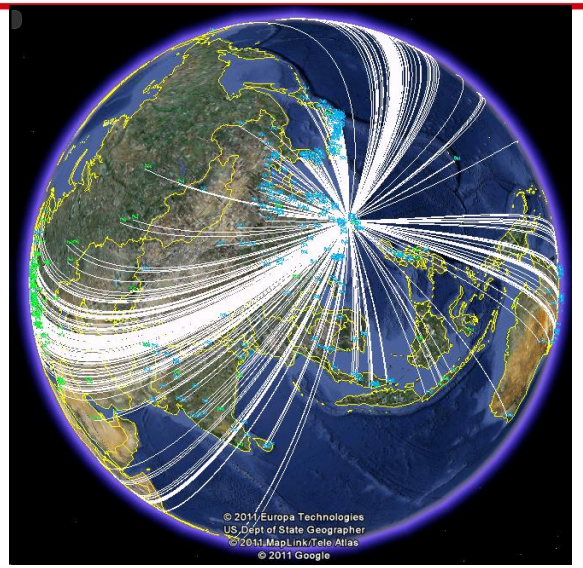
- 大多混合多種行為，包括病毒、蠕蟲、木馬或後門程式等特性
- 暱蹤技術的使用
  - Fast-Flux Domain
  - P2P
  - 加密通訊
  - 其它未被發現的…
- 目標
  - 感染主機、擴大領域、竊取資料

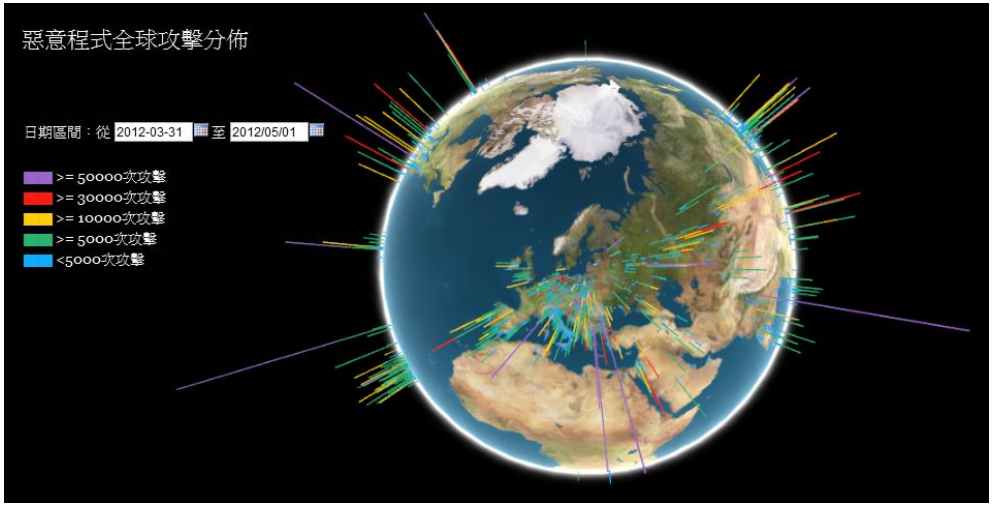
Bot & Botnet在那裏？

NARLabs

承諾·熱情·創新

- 使用者端的設備
  - 個人電腦
  - 行動裝置
- 網路設備
  - ADSL分享器
- 文件(APT攻擊時常用)
  - Office系列
  - PDF
  - 影音格式

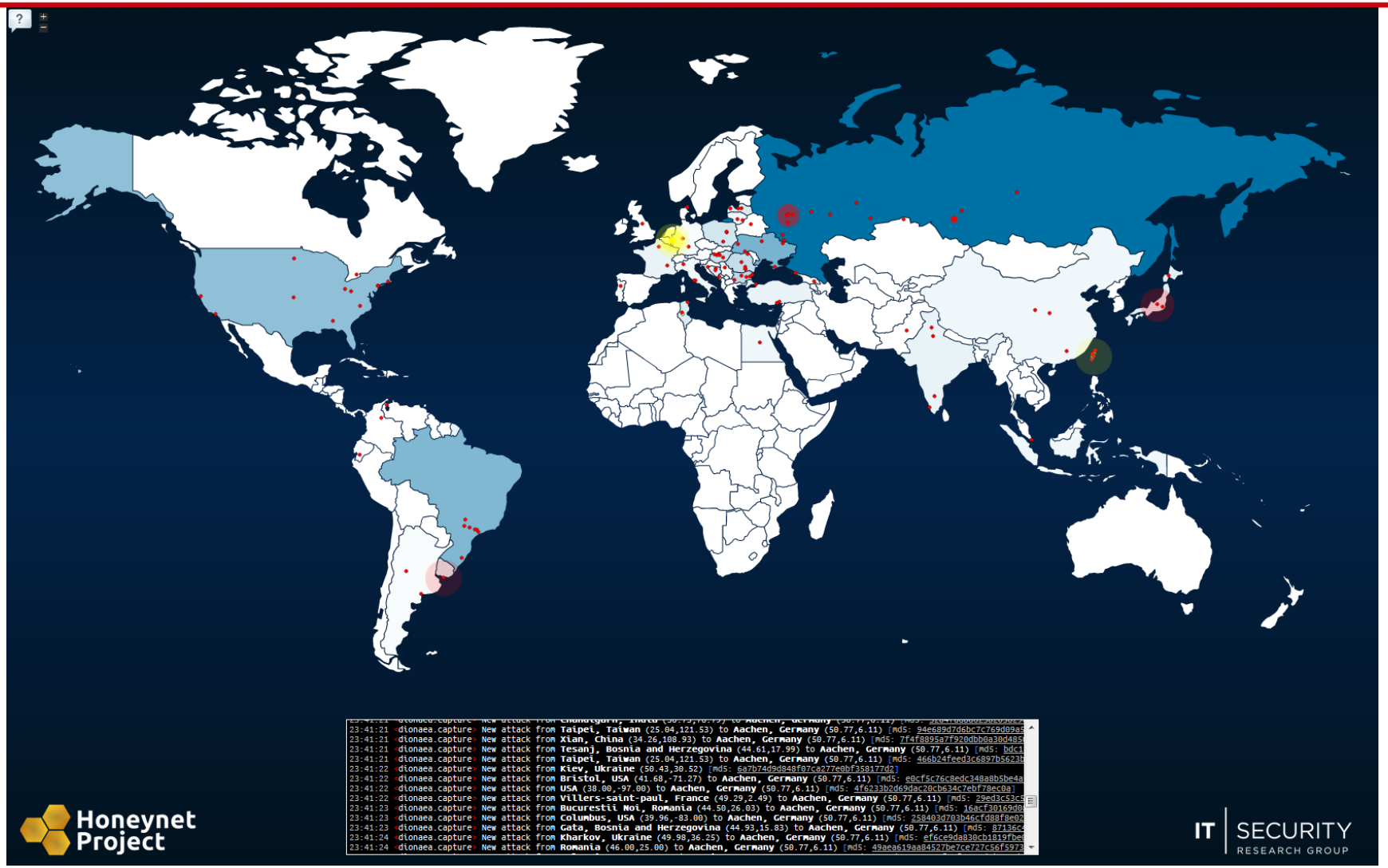




全球Botnet活動地圖

NARLabs

承諾·熱情·創新



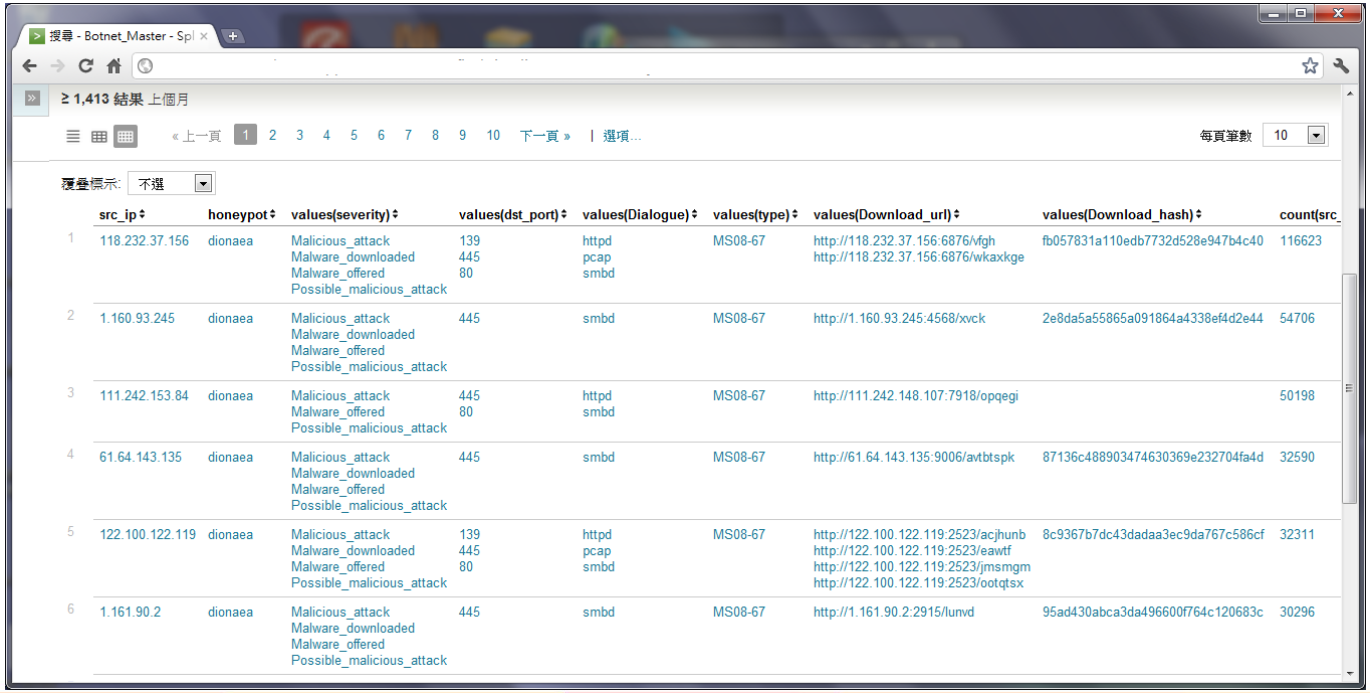
Source: The Honeynet Project Threat Map

巨量資訊分析

NARLabs

承諾·熱情·創新

- 日誌巨量成長快速，目前有分析價值的資料，約為2,500 EPS
- 分散式的搜尋各偵測點有價值的資訊
- 結合多種偵測系統
- 以資訊安全應變的角度，即時進行資訊的分析才有價值



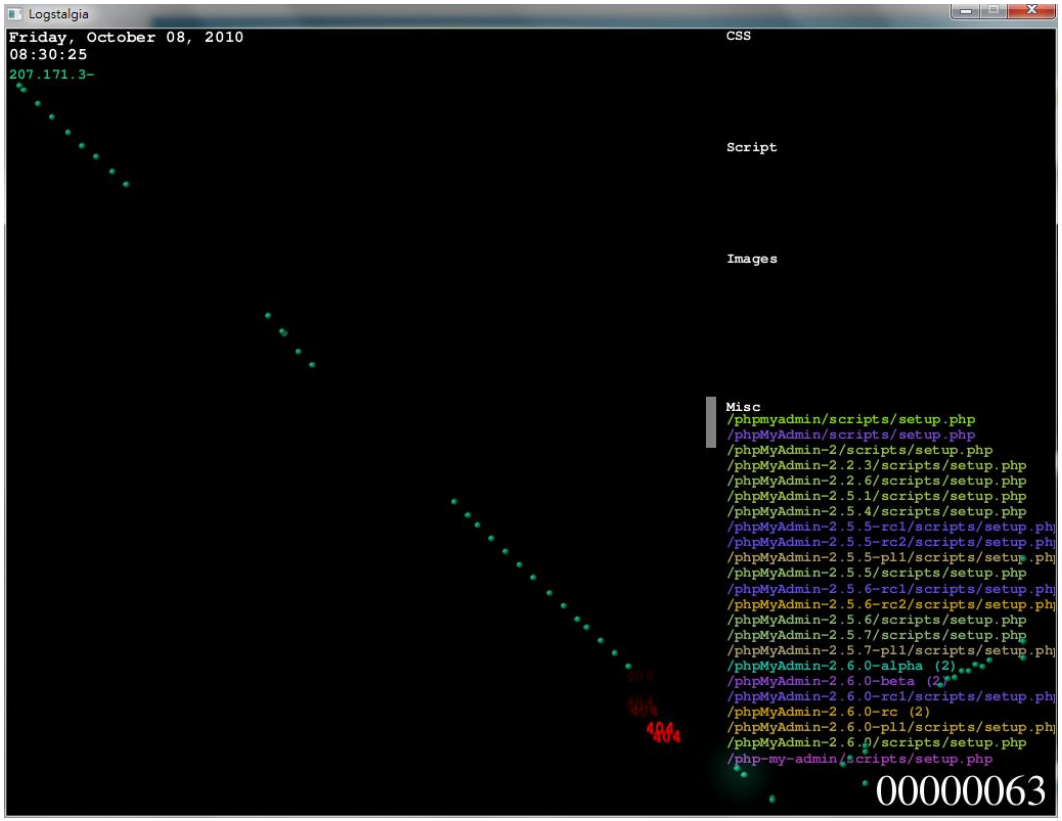
	src_ip	honeypot	values(severity)	values(dst_port)	values(Dialogue)	values(type)	values(Download_url)	values(Download_hash)	count(src_
1	118.232.37.156	dionaea	Malicious_attack Malware_downloaded Malware_offered Possible_malicious_attack	139 445 80	httpd pcap smbd	MS08-67	http://118.232.37.156:6876/vfgh http://118.232.37.156:6876/wkaxkge	fb057831a110edb7732d528e947b4c40	116623
2	1.160.93.245	dionaea	Malicious_attack Malware_downloaded Malware_offered Possible_malicious_attack	445	smbd	MS08-67	http://1.160.93.245:4568/xvck	2e8da5a55865a091864a4338ef4d2e44	54706
3	111.242.153.84	dionaea	Malicious_attack Malware_offered Possible_malicious_attack	445 80	httpd smbd	MS08-67	http://111.242.148.107:7918/opqegi		50198
4	61.64.143.135	dionaea	Malicious_attack Malware_downloaded Malware_offered Possible_malicious_attack	445	smbd	MS08-67	http://61.64.143.135:9006/avtbtspk	87136c488903474630369e232704fa4d	32590
5	122.100.122.119	dionaea	Malicious_attack Malware_downloaded Malware_offered Possible_malicious_attack	139 445 80	httpd pcap smbd	MS08-67	http://122.100.122.119:2523/acjhunb http://122.100.122.119:2523/eawtf http://122.100.122.119:2523/jmsmgm http://122.100.122.119:2523/ootqtsx	8c9367b7dc43dadaa3ec9da767c586cf	32311
6	1.161.90.2	dionaea	Malicious_attack Malware_downloaded Malware_offered Possible_malicious_attack	445	smbd	MS08-67	http://1.161.90.2:2915/lunvd	95ad430abca3da496600f764c120683c	30296

資料視覺化分析

NARLabs

承諾・熱情・創新

- Web services logs analysis
- Watching and finding



情資整合的重要

- 多樣化的偵測系統與資訊安全設備
- 分散式資料處理的複雜
- 巨量資料的關聯分析
- 偵測、分析與應變流程的自動化
- 資訊交換與分析中心

偵測與分析技術

- 掌握Botnet行蹤
  - 受害者
    - 系統異常狀態、惡意程式活動
  - 網路通訊
    - 微量通訊、巨量通訊
  - 中繼站/控制站
    - 網路連線數
  - 情資整合
    - 系統日誌、網路流量、資安設備比對、資料檔案等

全球Botnet活動地圖

NARLabs

承諾·熱情·創新

每日活動分析

每週活動分析

新型態Botnet之發展

- 潛伏期能夠進行管理，但必須降低網路流量異常的出現
- 避開端點防護軟體的特徵偵測
- 避開入侵偵測系統的比對
- 竊取使用者端的資料，送往資料集中站
- 自動化的更新惡意程式

行動裝置的惡意程式

NARLabs
承諾·熱情·創新

- 隱藏在看似正常的應用程式(APP)、網址連結中
- 背後截取行動裝置使用者的資料
- 透過網路的連結傳送到資料集中站

Personal information
Contacts
Social Network
Web services
Location
etc.

3G/WiFi

Mobile OS/Testbed

Advanced Currency Converter
App Uninstaller
Chess
Dice Roller
Falling Ball Dodge
Falling Down
Funny Paint
Hilton Sex Sound
Hot Sexy Videos
Photo Editor
Scientific Calculator
Screaming Sexy Japanese Girls
Spider Man
Super Guitar Solo
Super History Eraser
Super Ringtone Maker
Super Sex Positions
几何战机_PewPew
下坠滚球_Falldown
躲避弹球
蜘蛛侠

Android Market
Downloaded over 50,000 times.

行動裝置惡意程式的發展

- App Market
  - 應用程式更新時，才植入惡意程式
  - 要求更多的權限
- QR Code
  - 儲存資料
  - URL、TEXT、Phone Number、SMS等



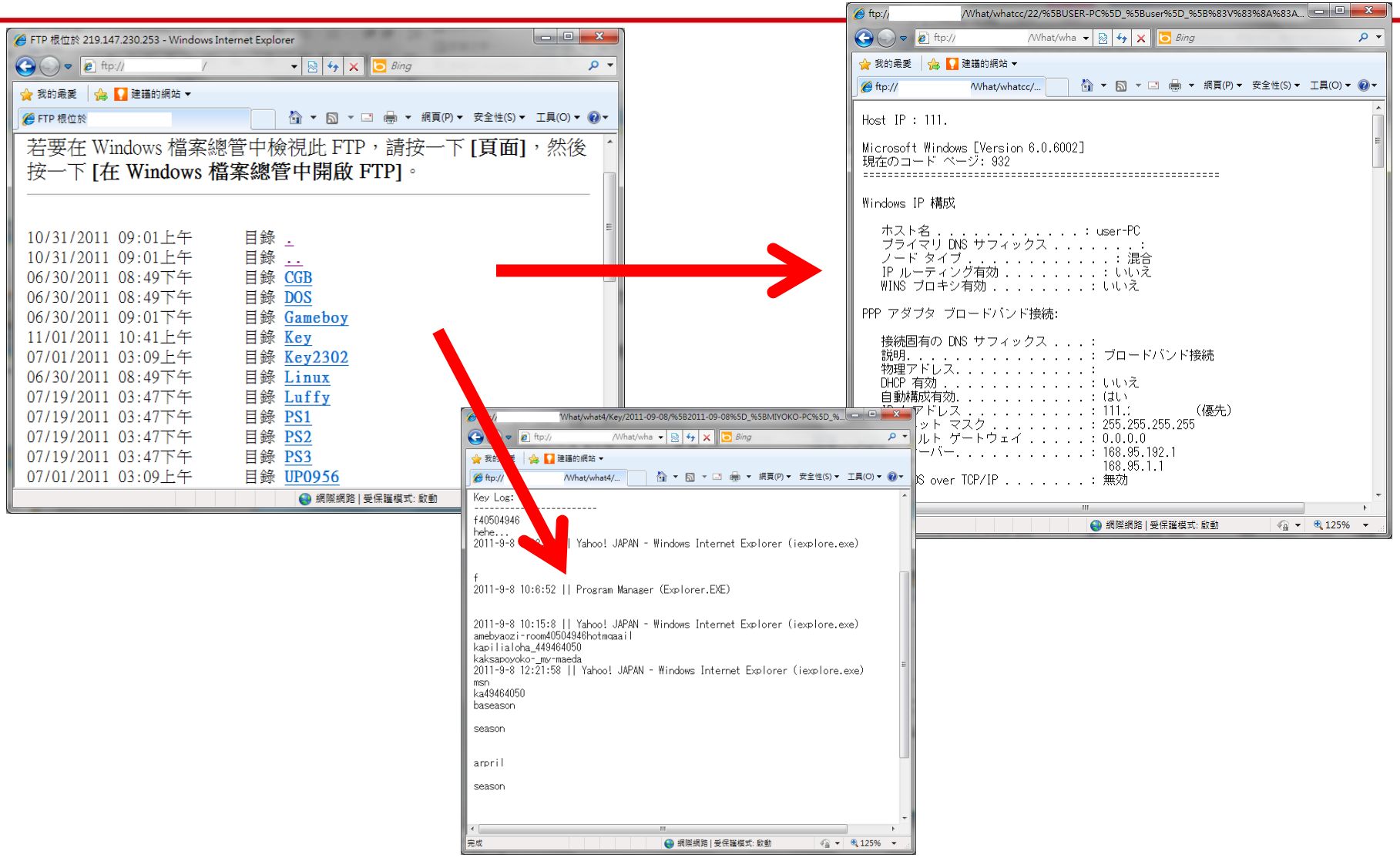

案例分享

- 從Hacker的角度思考
  - 加密通訊協定的弱點
  - 如何取得有用的資訊
  - 需要管理的主機眾多，如何建立自動化的回報機制而不被發現
  - 如何避開目前資安全設備的偵測機制
- 分享Botnet CC追蹤與分析
  - Keylogger Botnet

Botnet Mother Ship

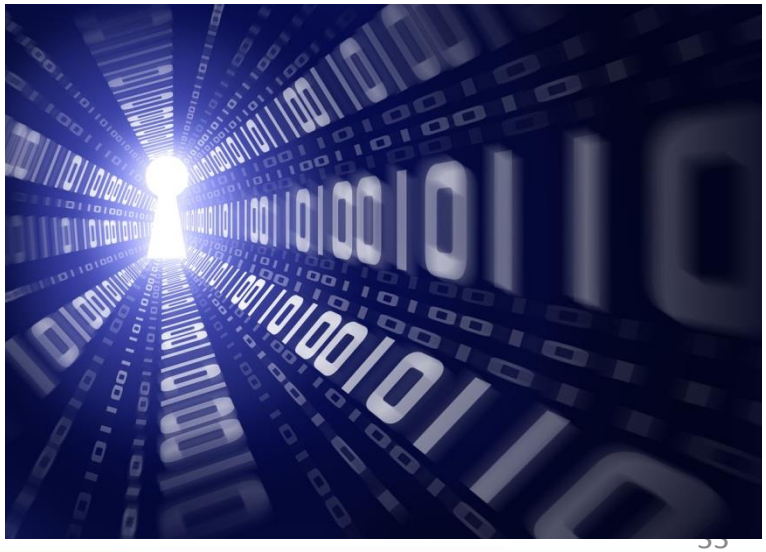
NARLabs

承諾・熱情・創新



結論

- 網路攻擊事件對於現有資訊環境造成直接影響
- 系統與設備管理人員需具備網路攻防技能
- Botnet已結合傳統多種攻擊手法，發展出獨有之技術
- 匿蹤技術提供Botnet活動更多的保護，追蹤上不易
- Key Logger與Spyware的活動，造成隱私資料外洩



- 蔡一郎 Steven Tsai
- yilang@nchc.narl.org.tw
- 06-5050940-749