BCCS 漢昕科技

長庚科技大學

106年度資訊安全宣導--**<<資訊安全基本認知>>**

一般人員教育訓練

漢昕科技股份有限公司
資安顧問 洪有志

簡報大綱

- 個資暨資安案例分享
- 2017年資安預測
- 釣魚郵件與網站介紹與防護
- 物聯網(IoT)資安
- 勒索軟體介紹與防護

簡報大綱

- 個資暨資安案例分享
- 2017年資安預測
- 釣魚郵件與網站介紹與防護
- 物聯網(IoT)資安
- 勒索軟體介紹與防護

智慧TV變竊聽器? 維基解密爆CIA監聽 20170309

資料來源：https://www.youtube.com/watch?v=J13yXCjDmYs

電郵疑遭攔截萬筆個資洩 外交部說明 20170208

資料來源：https://www.youtube.com/watch?v=7M1LPp_liFM

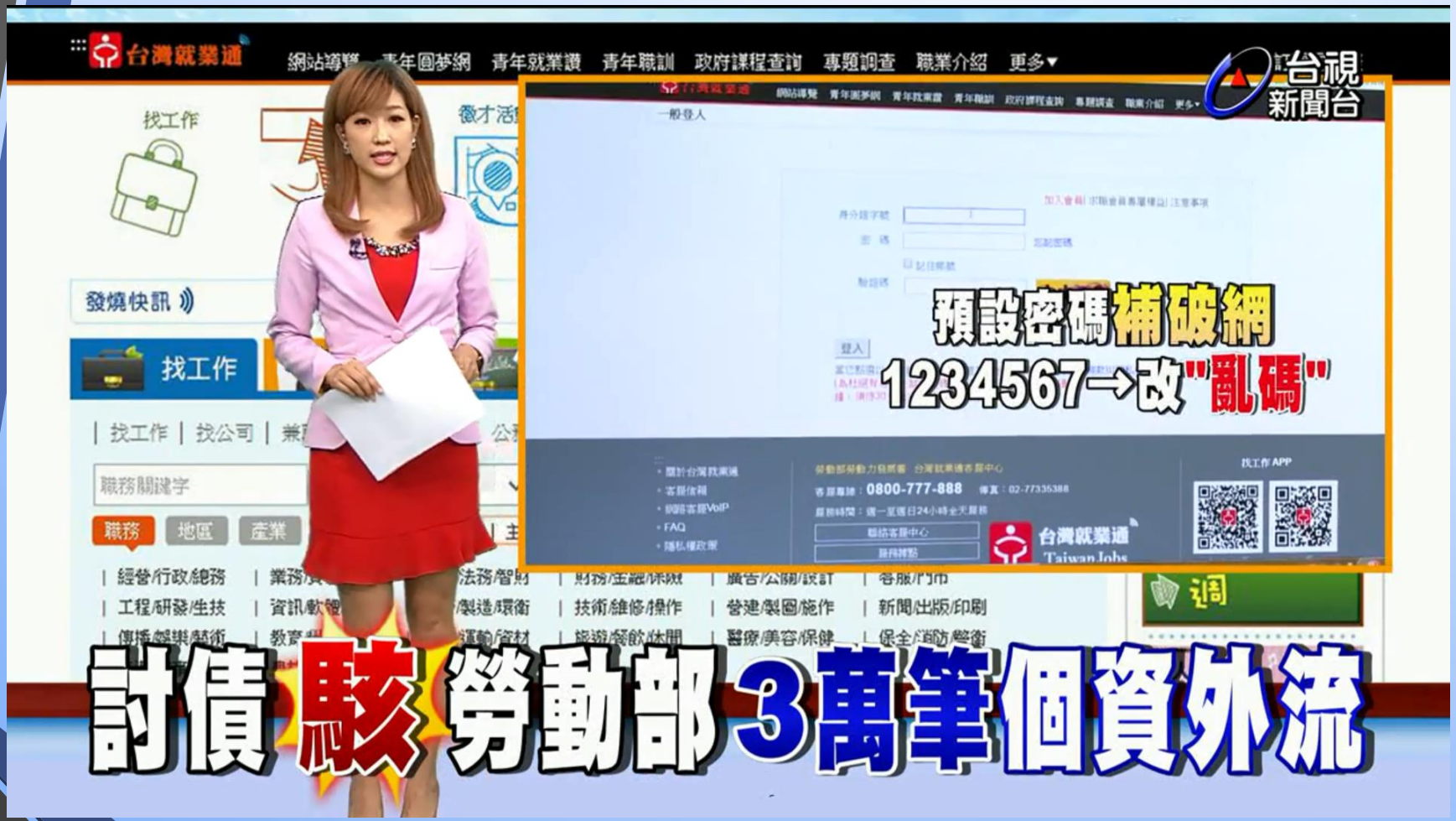
史上最大宗! 6券商集體遭駭客攻擊勒索 20170204

資料來源：https://www.youtube.com/watch?v=32o5EmCmIP0

北市府洩個資 員工薪資看光光 20170110

資料來源：https://www.youtube.com/watch?v=kTPfgpuTb18

駭客突襲勞部就業通3萬筆個資外流 20161026



資料來源：https://www.youtube.com/watch?v=-0CYXaqlUhs

駭客攻擊第一金證券系統 勒索比特幣 20160923

資料來源：https://www.youtube.com/watch?v=13ap4RS6uAY

一銀盜領案起訴! 三嫌各求處12年
20160914

資料來源：https://www.youtube.com/watch?v=C23a9PTCG0A

會員系統疑似個資外洩 兩廳院爆首起詐騙 20160901

資料來源：https://www.youtube.com/watch?v=GAQLw2NpUdI

中華郵政爆發個資外洩1.7萬筆
20160525

資料來源：https://www.youtube.com/watch?v=nRWjYGHyn9M

美資安專家: 2億7千萬信箱遭駭
20160504

資料來源：https://www.youtube.com/watch?v=gOYQb58Kf3Y

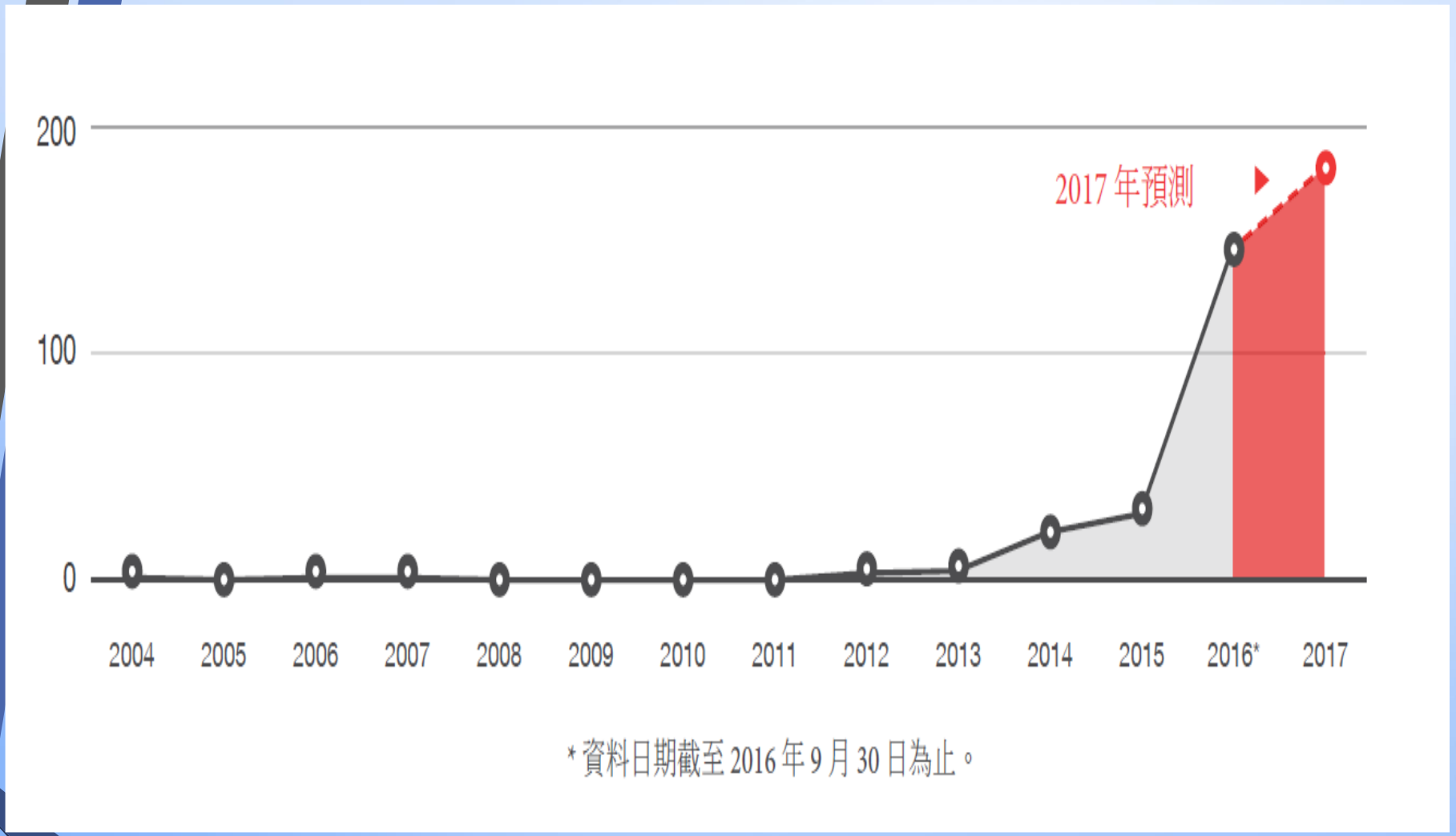
簡報大綱

- 個資暨資安案例分享
- 2017年資安預測
- 釣魚郵件與網站介紹與防護
- 物聯網(IoT)資安
- 勒索軟體介紹與防護

1. 2017 年勒索病毒成長力道將開始平緩，但攻擊手法將朝多元化發展。

- 新的勒索病毒家族數量成長率將在 25% 左右，平均每個月約出現 15 個新的家族。由於勒索病毒的高峰期在 2016 年已過，因此在進入穩定期之後，歹徒將朝著多元化發展，讓病毒蔓延至更多潛在受害者、平台與更大的攻擊目標。
- 勒索病毒將成為資料外洩事件中的常客。
- 行動勒索病毒預料將追隨桌上型電腦勒索病毒的發展腳步。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技



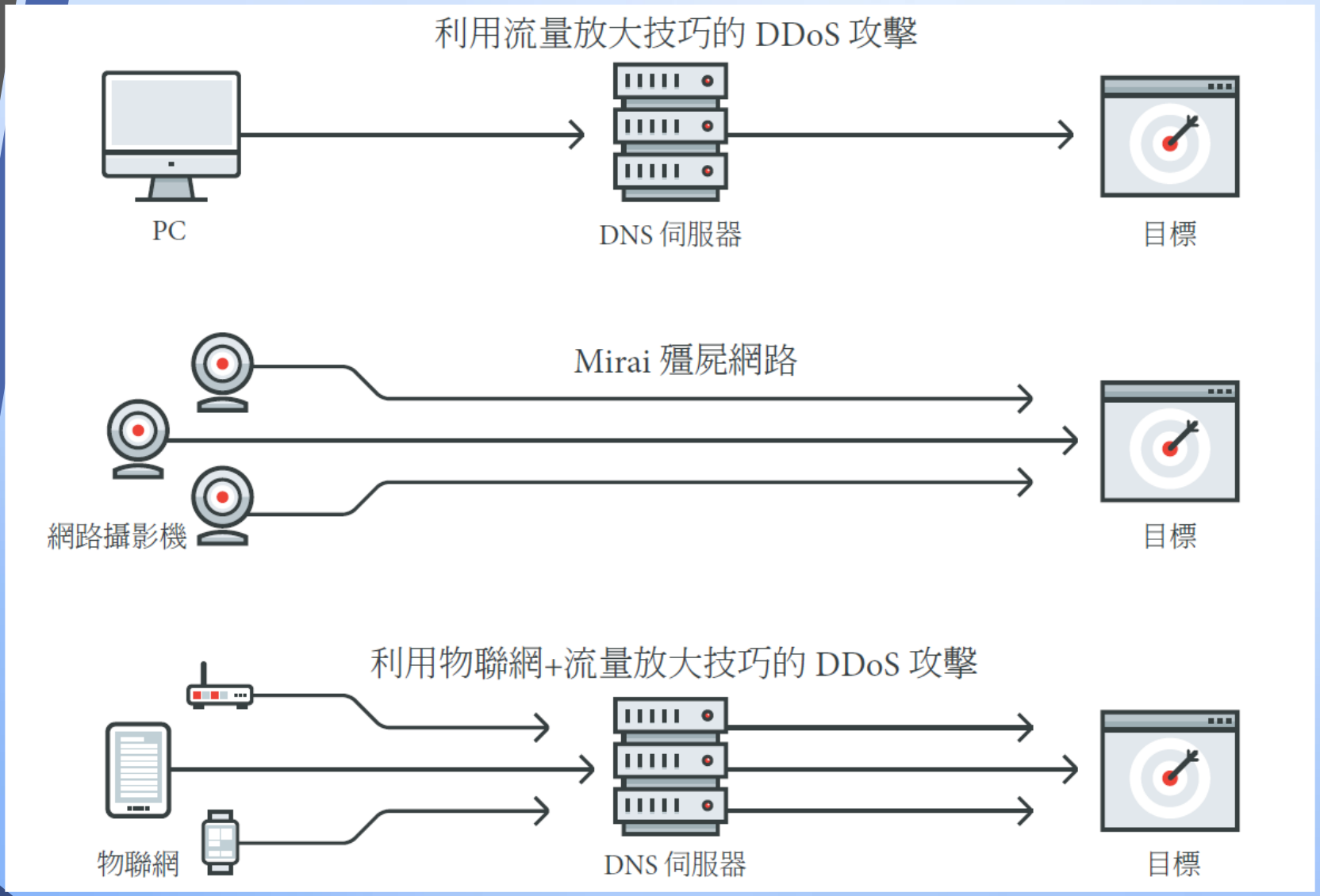
◆ 勒索病毒家族逐年數量 (含 2017 年預測)。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

2. 物聯網裝置將在分散式阻斷服務(DDoS)攻擊當中扮演更大的角色，而工業物聯網系統也將成為針對性攻擊的目標。

- 網路犯罪集團將使用類似 Mirai 殭屍網路的惡意程式來發動 DDoS 攻擊。
- 從 2017 年起，一些服務導向、新聞、企業和政治相關的網站，將遭到有系統的大規模 HTTP 流量攻擊。
- 廠商將無法及時阻止這類攻擊發生。
- 工業物聯網的發展趨勢將為企業帶來前所未有的資安危機和風險，並且連帶影響消費者。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技



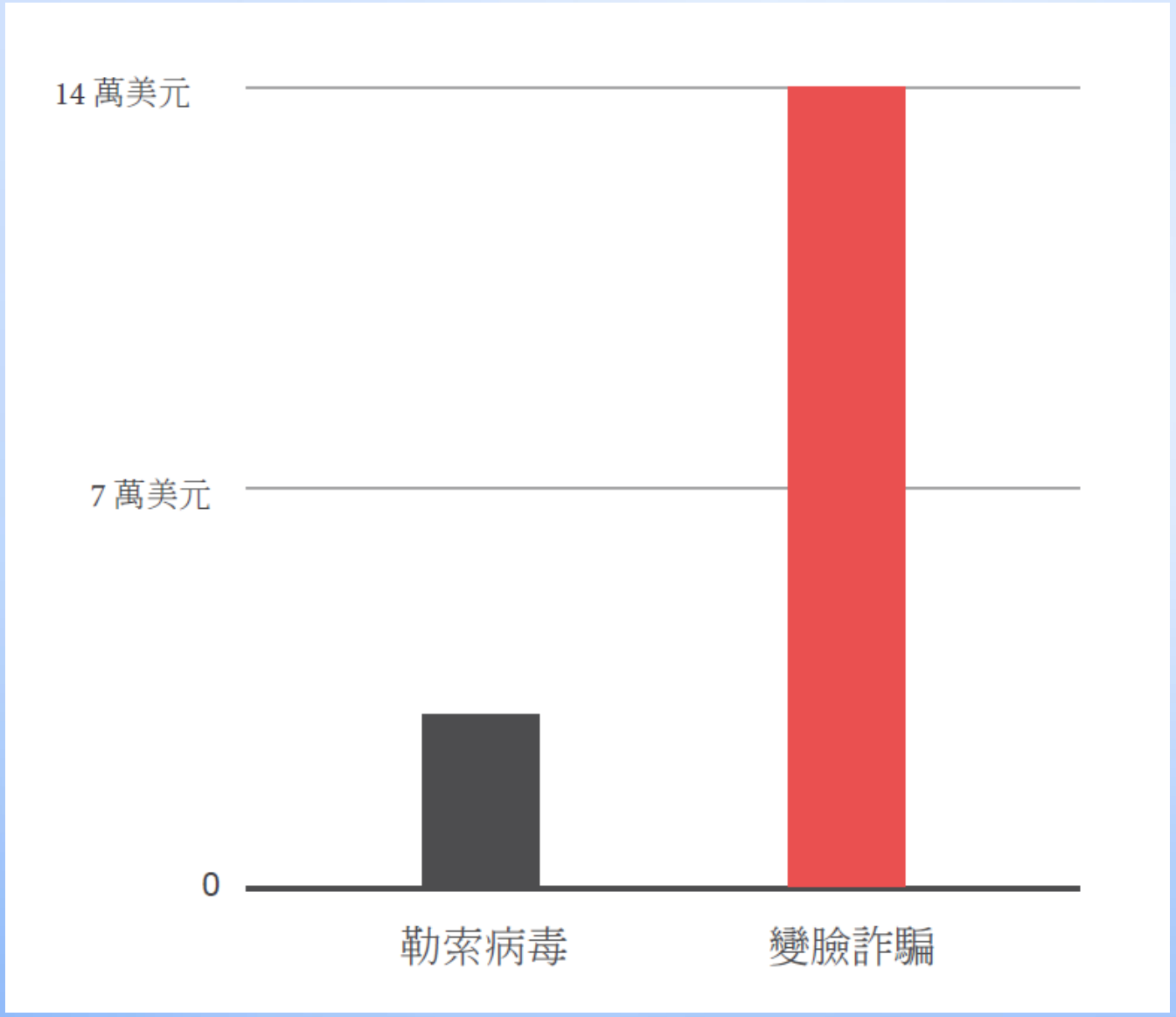
- Mirai 殭屍網路不需使用 DNS 伺服器來癱瘓目標，但仍足以讓許多使用者無法連上目標網站。理論上，物聯網殭屍網路也能發動流量放大技巧來發動 DDoS 攻擊，並且造成更大傷害。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

3. 變臉詐騙太容易得逞將使得 2017 年的針對性詐騙數量增加。

- 專門以全球企業財務部門為攻擊目標的「變臉詐騙」，其手法是先駭入某個電子郵件帳號，然後再透過該帳戶指使員工將一筆款項匯到歹徒的銀行帳戶。
- 由於變臉詐騙太過容易得逞，尤其是假冒執行長的詐騙，因此將成為網路犯罪集團最愛的詐騙手法之一。
- 變臉詐騙郵件特別不容易偵測，因為這類郵件並未挾帶惡意程式或執行檔。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技



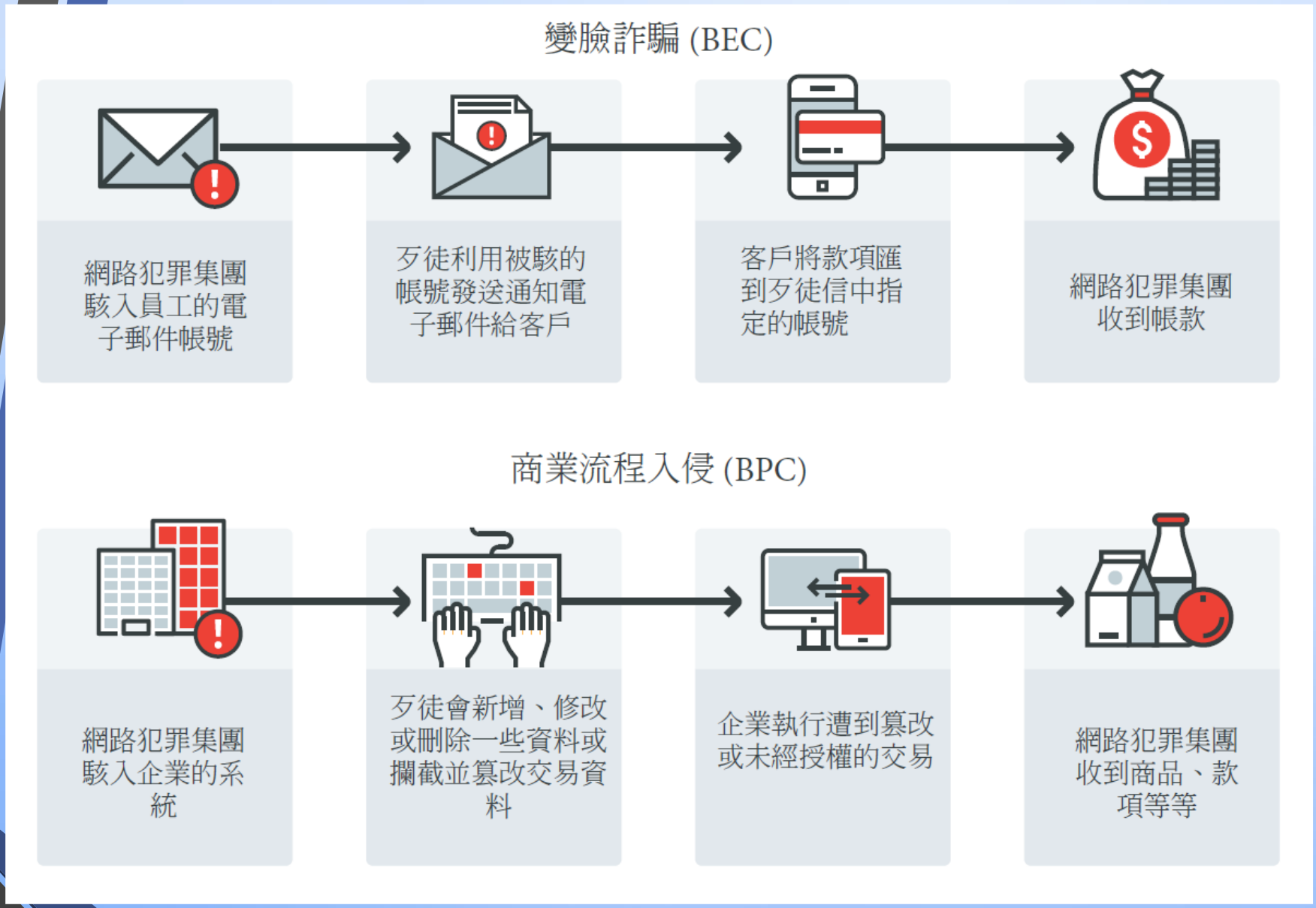
◆ 勒索病毒攻擊與變臉詐騙企業平均損失金額比較。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

4. 商業流程入侵將逐漸獲得網路犯罪集團青睞，目標將鎖定財務相關部門。

- 歹徒的最終目標仍是將資金匯出，但「商業流程入侵」(Business Process Compromise，簡稱 BPC)的攻擊對象並不侷限於財務部門。
- BPC攻擊平均不法潛在獲利為 8,100 萬美元。
- 可能的攻擊手法包括：
  - 駭入採購系統，進而暗中攔截原本應該匯給廠商的款項。
  - 駭入付款流程系統也能收到類似效果。
  - 駭入出貨中心的電腦系統，將高價值的商品轉寄至歹徒指定的地點。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技



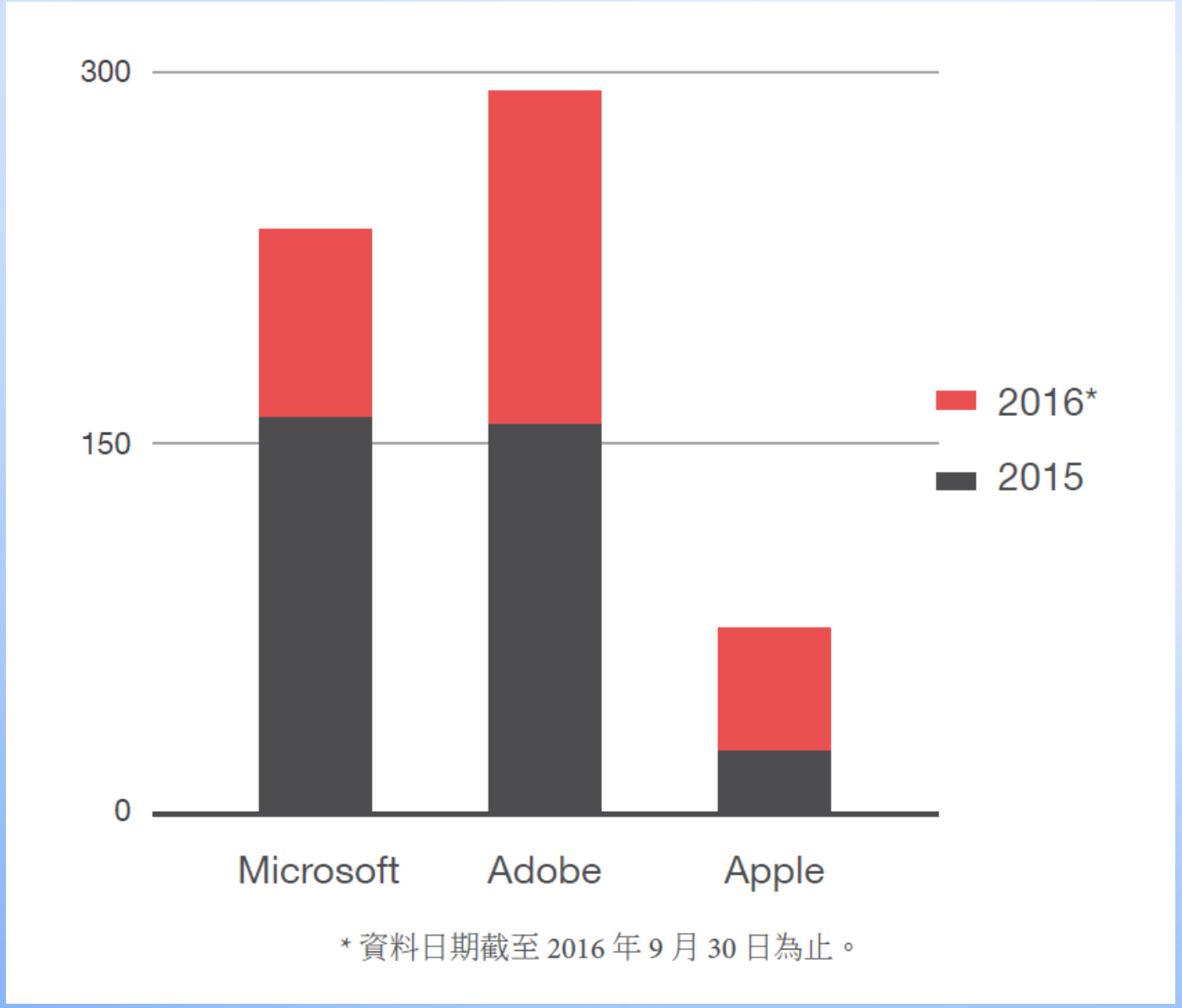
◆ BEC 和 BPC 攻擊過程比較。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

5. Adobe 和 Apple 平台新發現的漏洞數量將超越 Microsoft。

- 因為 Windows PC 出貨量近年來持續衰退之外，另一項因素是有越來越多使用者平常使用智慧型手機或商用平板而非一般電腦。
- 所有的 Adobe 漏洞最後都會被收錄到漏洞攻擊套件當中。
- 購買 Mac 電腦的消費者越來越多，歹徒的目光就會開始轉向 Apple 的軟體漏洞。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技



◆ ZDI 漏洞懸賞計畫所揭露的 Microsoft、Adobe 和 Apple 漏洞。

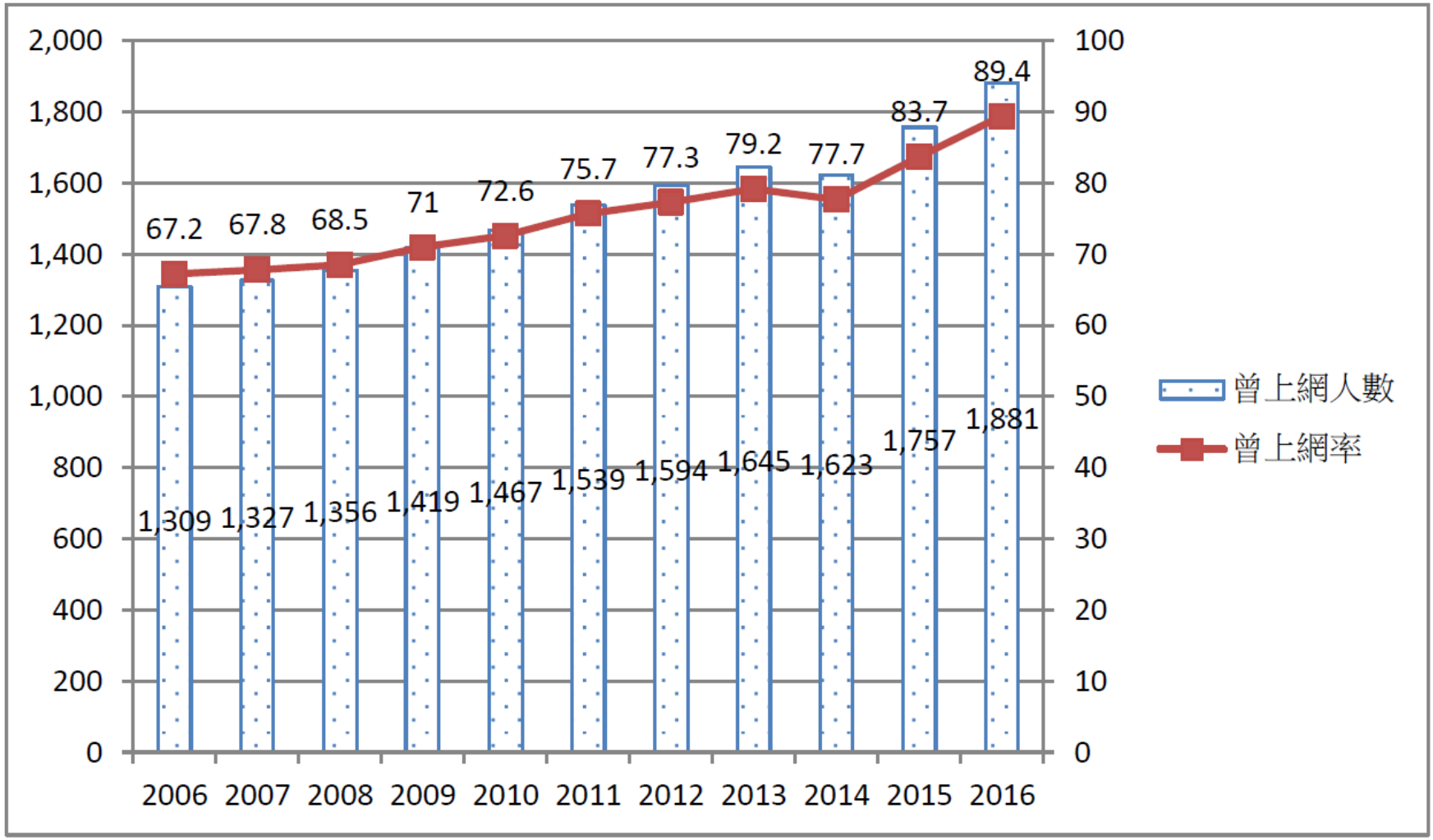
資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

6. 網路宣傳將成為一種常態。

- 2016 年全球將近半數的人口 (46.1%) 都已能連上網際網路，不論是透過智慧型手機、傳統電腦或網際網路資訊站。
- 這表示越來越多人能夠輕易取得各種資訊，不論資訊的來源和可信度如何。
- 由於網路資訊缺乏審查機制，因而難以辨別真偽。
- 社群媒體的使用、濫用及誤用的情況勢必更加普遍，任何人只要能夠策略性運用這類手法來左右大眾輿論，就可能創造出對自己有利的結果。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

單位：萬人/%



◆ 台灣12 歲以上民眾曾經上網行為趨勢分析。

資料來源：歷年個人及家庭上網行為趨勢分析，財團法人台灣網路資訊中心

7. 「通用資料保護法規」的上路，將使得企業機構的管理成本增加。

- 歐盟即將上路的「通用資料保護法規」(GDPR) 不僅適用歐盟會員國，凡是需要蒐集、處理和儲存歐盟人民個人資料的全球企業機構都將適用。
- 2018 年，當該法規正式上路時，違反的企業最高將可能受到該公司全球營收 4% 的罰鍰。
- GDPR 將掀起一波企業政策和流程的變革，並且大幅提高企業管理成本。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

8. 歹徒將開發出能夠躲避今日偵測技術的最新針對性攻擊手法。

- 歹徒將採取更多能夠躲避現代化資安技術的方法。例如，過去駭客大多使用執行檔，後來改用文件檔案，而現在則是較常使用腳本和批次檔。
- 運用一些更複雜的沙盒偵測技巧，並且觀察目標網路是否會將未知檔案傳送至沙盒模擬環境當中分析，甚至會攻擊沙盒環境，讓沙盒模擬分析失去作用。
- 虛擬機器規避 (VM Escape) 的技巧將成為進階漏洞攻擊程序當中備受重視的元素。

資料來源：資安攻防新層次_趨勢科技 2017 年資安預測，趨勢科技

簡報大綱

- 個資暨資安案例分享
- 2017年資安預測
- 釣魚郵件與網站介紹與防護
- 物聯網(IoT)資安
- 勒索軟體介紹與防護

社交工程郵件的APT攻擊事件分析

From: [redacted]秘書室<jungte.wu@msa.hinet.net>
To: [redacted]@ms35.hinet.net>
Date: Wed, 06 Apr 2016 08:56:39
Subject: [redacted]會員服務提升

本會會員\團體會員:

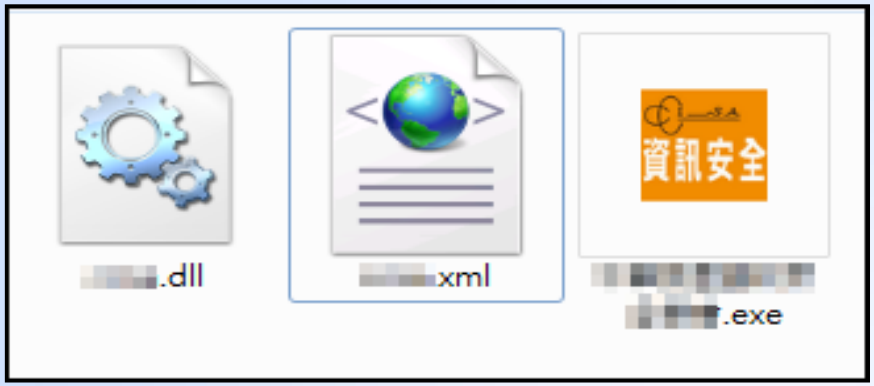
為提升會員服務,本會研發會員服務登錄系統以利舉辦與資訊安全相關之學術會議和舉行有關資訊安全之學術研究、講習、訓練 、討論、訪問、觀摩等活動事項之日程安排,詳情見附檔[redacted]會員服務登錄系統軟體。

軟體壓縮包解壓碼:888888
登錄默認密碼:[redacted]@2016

[redacted]學會.rar

[redacted]秘書室
秘書：[redacted]
地 址：[redacted]
電 話：[redacted]
地點：[redacted]

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心



SHA256: c5c32da2834a3c71e2d51f0d00b6887ee8268f847a0455594bac480ce0a31b93

File name: c .exe

Detection ratio: 3 / 57

Analysis date: 2016-05-04 10:04:15 UTC (5 days, 16 hours ago)

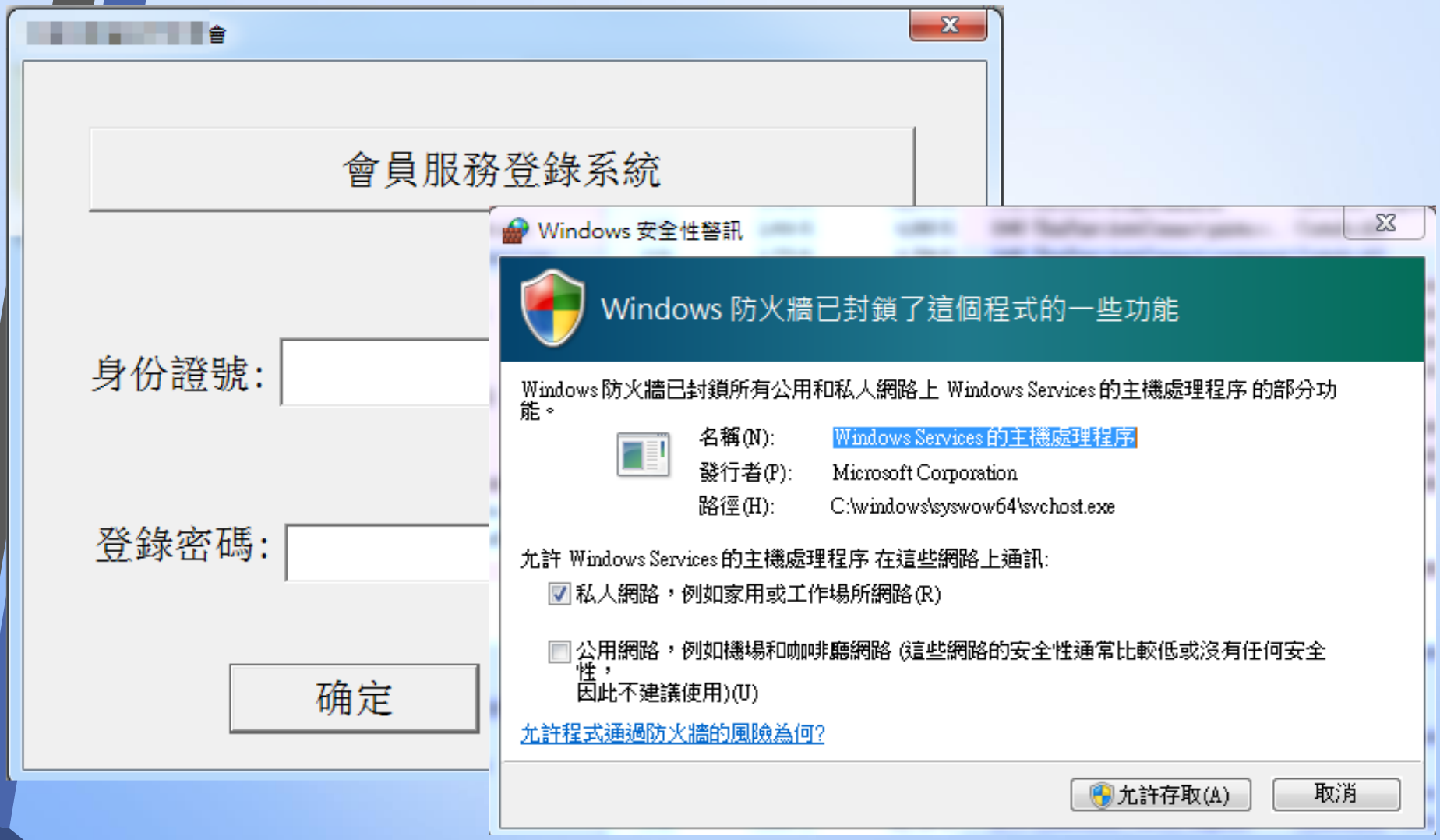
0 0

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
Avira (no cloud)	TR/Agent.Y.857	20160504
Ikarus	Trojan.Agent	20160504
McAfee-GW-Edition	BehavesLike.Win32.Downloader.dh	20160503

- 壓縮檔內分別是dll、xml和exe執行檔，且檔案名稱都是以該單位名稱命名。
- 該程式被偵測出的比例相當低 3/57 ， 算是客製化的惡意程式。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心



- 尚未輸入任何資料以前，防火牆就已經出現外部網路存取權限要求。
- 實際隨意輸入身分證號以及指定的登錄密碼，該程式會開啟瀏覽器並且連結至該單位的官方網站。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心

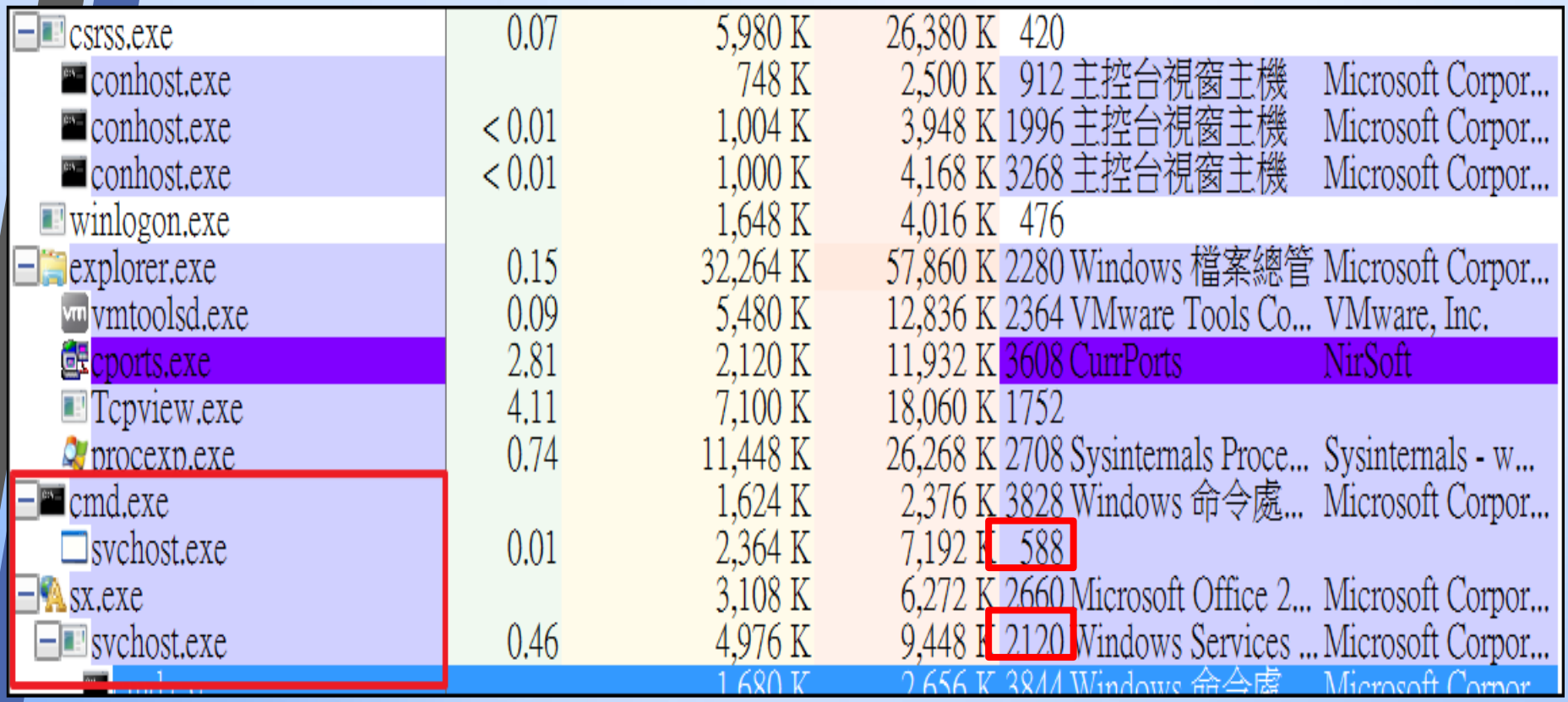
TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local P...	Remote Address	Remote...	State
services.exe	512	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING
services.exe	512	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	716	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING
svchost.exe	804	TCP	0.0.0.0	49153	0.0.0.0	0	LISTENING
svchost.exe	872	TCP	0.0.0.0	49154	0.0.0.0	0	LISTENING
svchost.exe	1016	UDP	0.0.0.0	123	*	*	
svchost.exe	1256	UDP	0.0.0.0	5355	*	*	
svchost.exe	716	TCPV6	[0:0:0:0:0:0:0:0]	135	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	804	TCPV6	[0:0:0:0:0:0:0:0]	49153	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	872	TCPV6	[0:0:0:0:0:0:0:0]	49154	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	1016	UDPV6	[0:0:0:0:0:0:0:0]	123	*	*	
svchost.exe	1256	UDPV6	[0:0:0:0:0:0:0:0]	5355	*	*	
svchost.exe	588	TCP	140.	49233	104.202.173.64	80	ESTABLISHED
svchost.exe	2120	TCP	0.0.0.0	1357	0.0.0.0	0	LISTENING
svchost.exe	2120	UDP	0.0.0.0	1357	*	*	
svchost.exe	2120	TCP	140.	49482	207.226.137.88	80	ESTABLISHED
svchost.exe	2120	TCP	140.	49486	207.226.137.88	80	ESTABLISHED
svchost.exe	2120	TCP	140.	49520	140	1357	SYN_SENT
svchost.exe	2120	UDP	0.0.0.0	60625	*	*	

- 大量的網路行為正在產生，都是透過名稱為 svchost.exe 的惡意程式進行(紫色部分)。

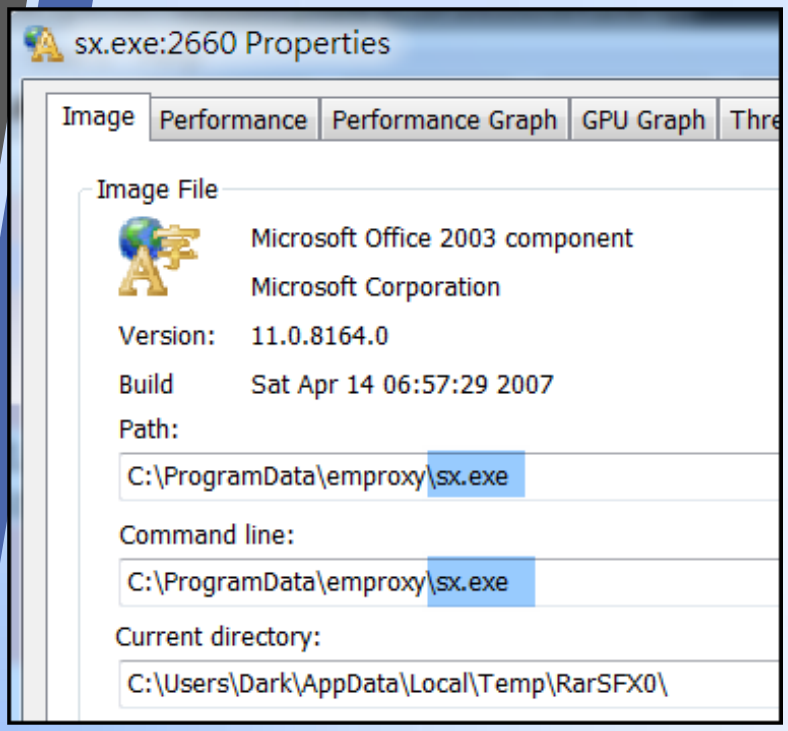
資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心

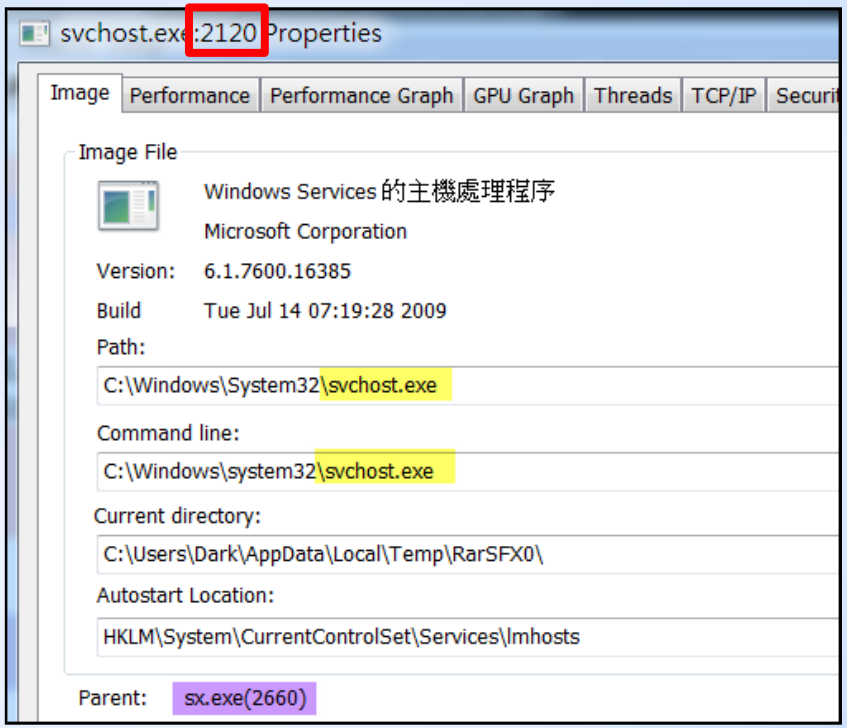


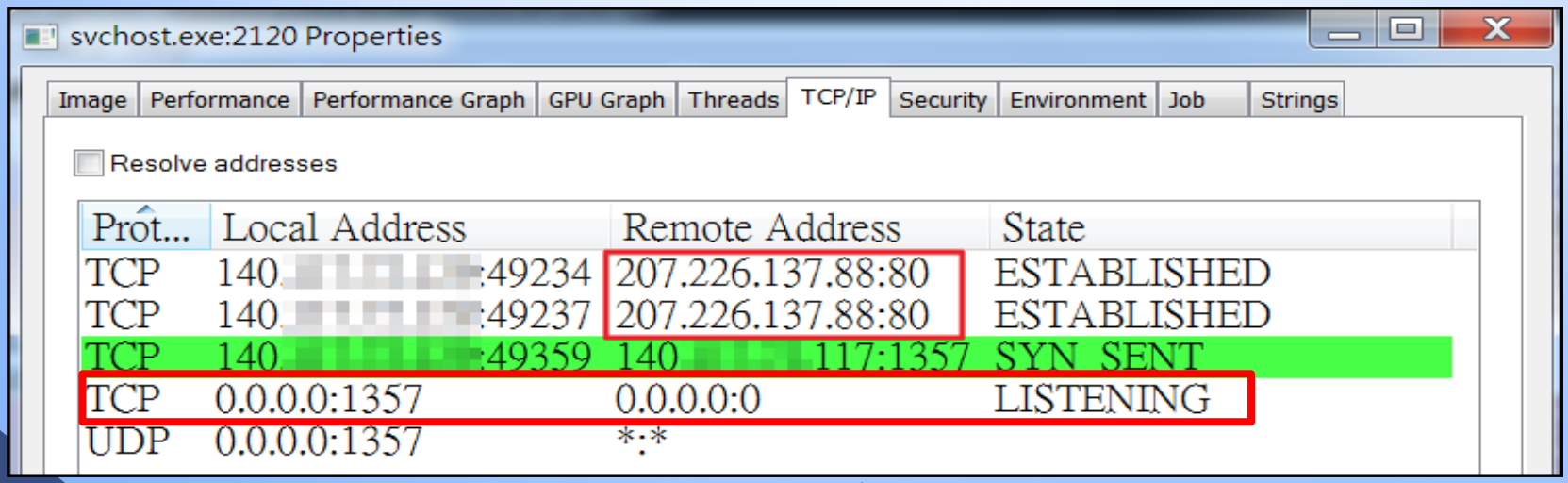
csrss.exe	0.07	5,980 K	26,380 K	420		
conhost.exe		748 K	2,500 K	912 主控台視窗主機	Microsoft Corpor...	
conhost.exe	< 0.01	1,004 K	3,948 K	1996 主控台視窗主機	Microsoft Corpor...	
conhost.exe	< 0.01	1,000 K	4,168 K	3268 主控台視窗主機	Microsoft Corpor...	
winlogon.exe		1,648 K	4,016 K	476		
explorer.exe	0.15	32,264 K	57,860 K	2280 Windows 檔案總管	Microsoft Corpor...	
vmtoolsd.exe	0.09	5,480 K	12,836 K	2364 VMware Tools Co...	VMware, Inc.	
cports.exe	2.81	2,120 K	11,932 K	3608 CurrPorts	NirSoft	
Tcpview.exe	4.11	7,100 K	18,060 K	1752		
procexp.exe	0.74	11,448 K	26,268 K	2708 Sysinternals Proce...	Sysinternals - w...	
cmd.exe		1,624 K	2,376 K	3828 Windows 命令處...	Microsoft Corpor...	
svchost.exe	0.01	2,364 K	7,192 K	588		
sx.exe		3,108 K	6,272 K	2660 Microsoft Office 2...	Microsoft Corpor...	
svchost.exe	0.46	4,976 K	9,448 K	2120 Windows Services ...	Microsoft Corpor...	
[illegible]		1,680 K	2,656 K	3844 Windows 命令處	Microsoft Corpor	

◆ 兩支異常的程式正在執行，檔案名稱都是 scvhost.exe 。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心

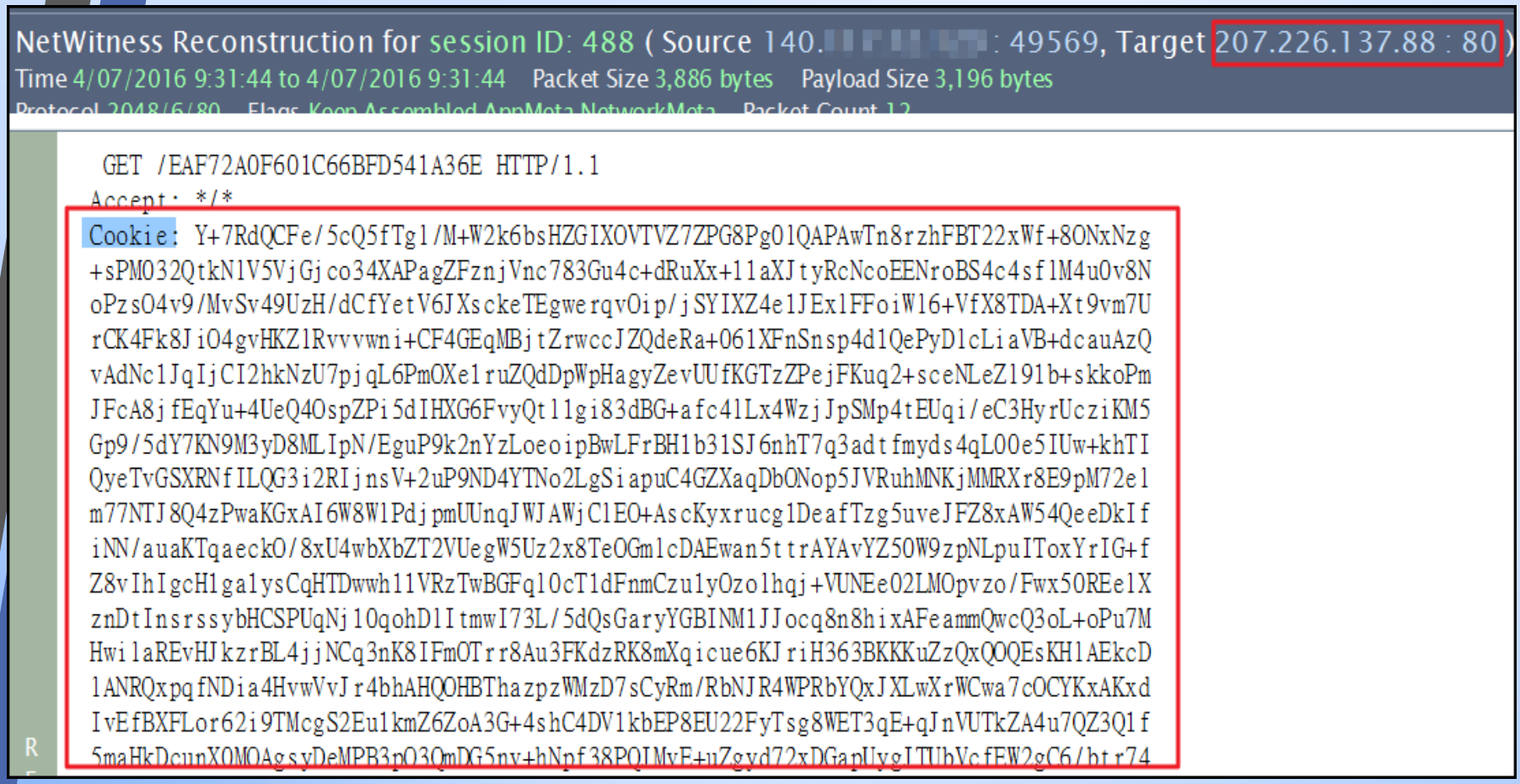






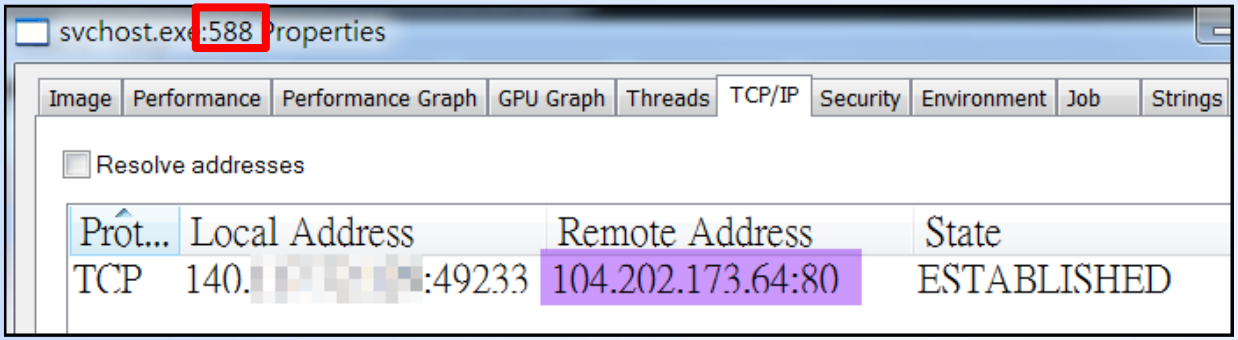
- PID 2120 的 svchost.exe 進行網路連線，目的端為 207.226.137.88 的 port 80 ，並開啟 TCP port 1357 接收 C&C 指令 。

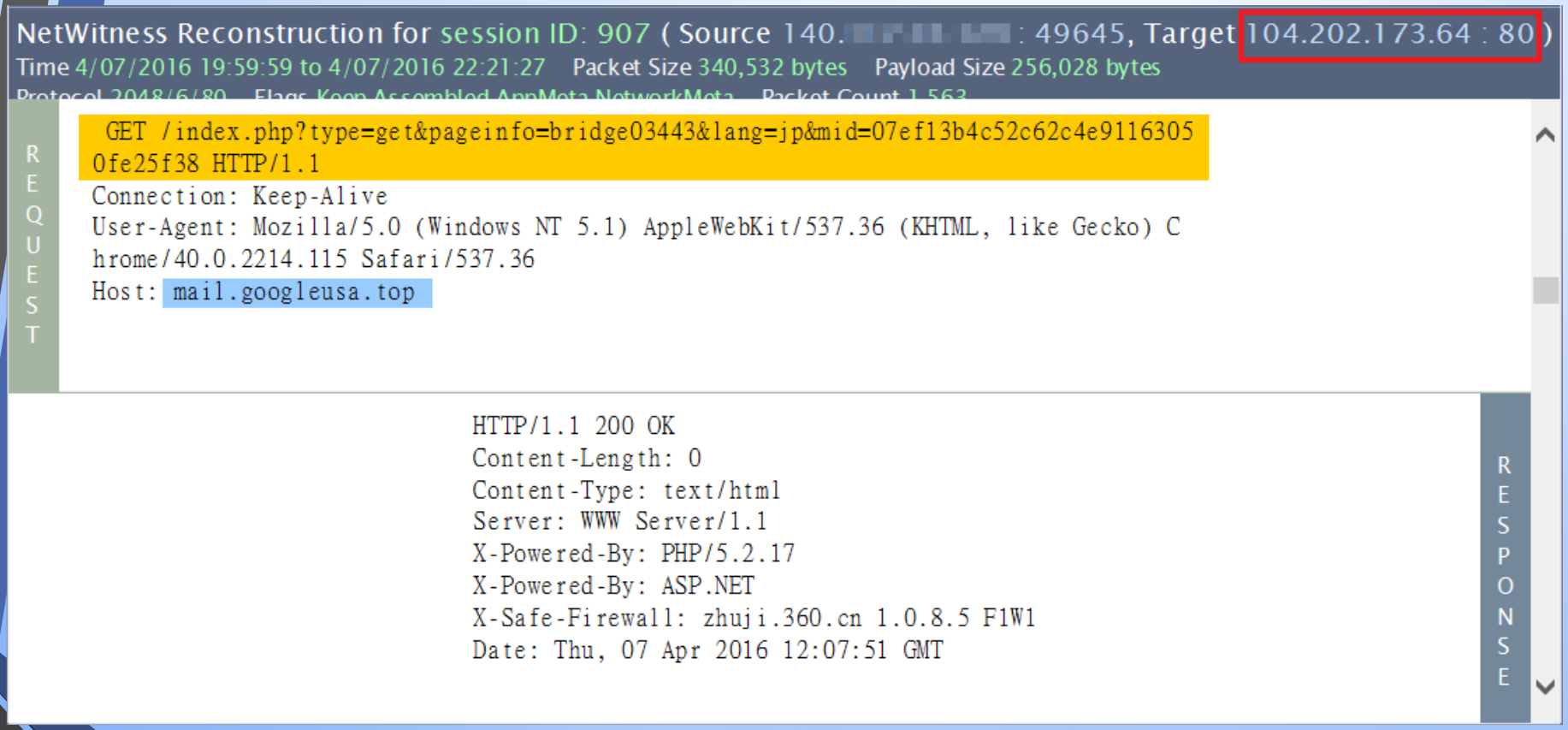
資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心



- IP 位址 207.226.137.88 ，為位於美國的 IP ，且直接透過瀏覽器無法開啟，應為駭客回報用的 C&C 主機。
- 該連線的封包資料都是以 HTTP GET 方式將資料送到 207.226.137.8 8的 port 80 接收，且疑似將竊取的資訊加密塞入 cookie 欄位傳送。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心





- 另一個 PID 588 的 svchost.exe ，固定網路連線至美國的 104.202.173.64 :80 ，然而該網址透過瀏覽器也是無法開啟，從回傳參數來看應該是在做回報的動作 。

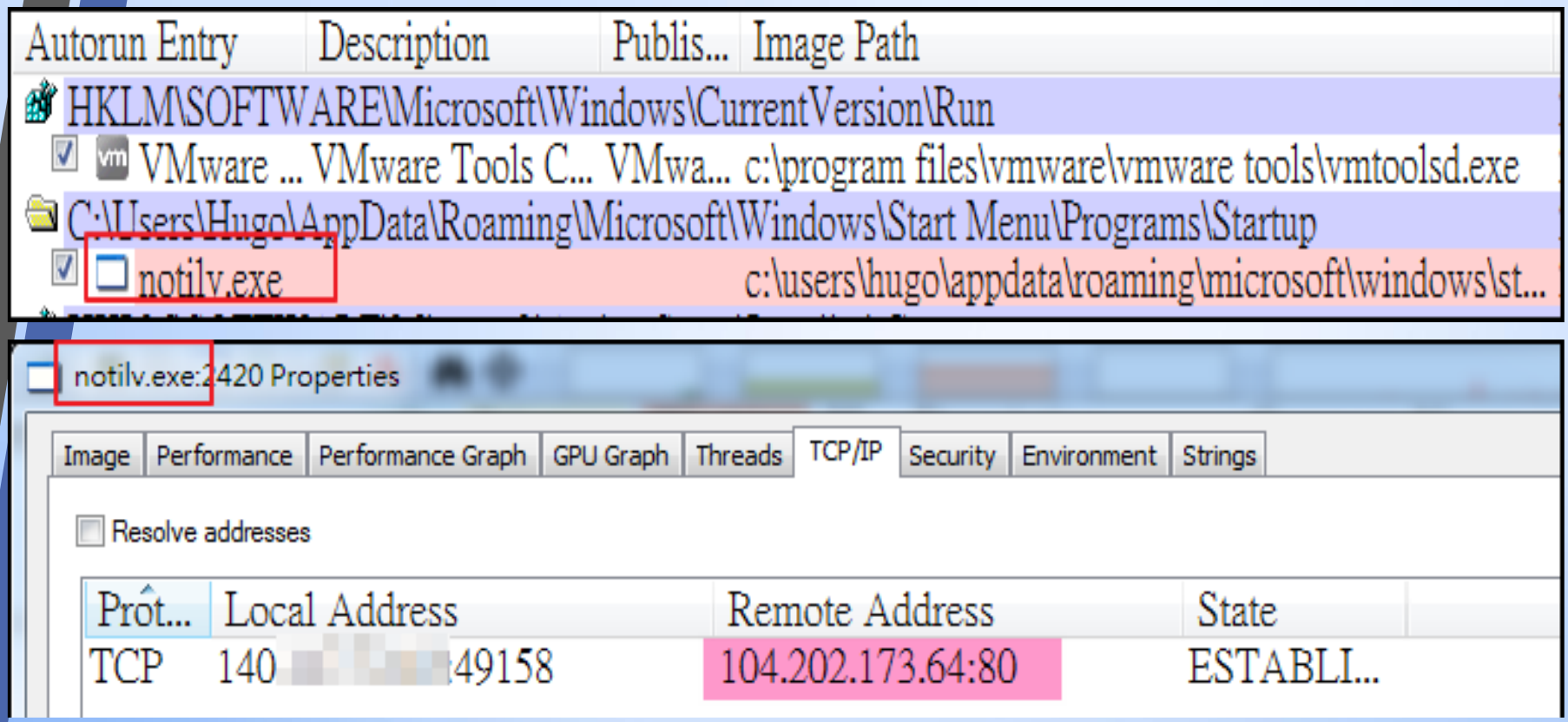
資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心

2016/4/7 上午 09:18:32	Added	svchost.exe	TCP 140. :49259	140. .17:1357
2016/4/7 上午 09:18:32	Removed	svchost.exe	TCP 140. :49258	140. .16:1357
2016/4/7 上午 09:18:34	Added	svchost.exe	TCP 140. :49260	140. .18:1357
2016/4/7 上午 09:18:34	Removed	svchost.exe	TCP 140. :49259	140. .17:1357
2016/4/7 上午 09:18:36	Added	svchost.exe	TCP 140. :49261	140. .19:1357
2016/4/7 上午 09:18:36	Removed	svchost.exe	TCP 140. :49260	140. .18:1357
2016/4/7 上午 09:18:38	Added	svchost.exe	TCP 140. :49262	140. .20:1357
2016/4/7 上午 09:18:38	Removed	svchost.exe	TCP 140. :49261	140. .19:1357
2016/4/7 上午 09:18:40	Added	svchost.exe	TCP 140. :49263	140. .21:1357
2016/4/7 上午 09:18:40	Removed	svchost.exe	TCP 140. :49262	140. .20:1357
2016/4/7 上午 09:18:43	Removed	svchost.exe	TCP 140. :49263	140. .21:1357

Time	Service	Size	Events		
2016-Apr-07 09:23:07	IP / UDP / OTHER	234 B	140.	-> 140. 113	62998 -> 1357
2016-Apr-07 09:23:21	IP / UDP / OTHER	234 B	140.	-> 140. 118	59612 -> 1357
2016-Apr-07 09:23:44	IP / UDP / OTHER	234 B	140.	-> 140. 126	58437 -> 1357
2016-Apr-07 09:24:10	IP / UDP / OTHER	234 B	140.	-> 140. 136	53359 -> 1357
2016-Apr-07 09:24:27	IP / UDP / OTHER	234 B	140.	-> 140. 142	56505 -> 1357
2016-Apr-07 09:24:50	IP / UDP / OTHER	234 B	140.	-> 140. 150	53766 -> 1357
2016-Apr-07 09:25:16	IP / UDP / OTHER	234 B	140.	-> 140. 159	60724 -> 1357
2016-Apr-07 09:25:42	IP / UDP / OTHER	234 B	140.	-> 140. 168	52355 -> 1357
2016-Apr-07 09:25:47	IP / UDP / OTHER	234 B	140.	-> 140. 170	64958 -> 1357
2016-Apr-07 09:25:49	IP / UDP / OTHER	234 B	140.	-> 140. 171	58039 -> 1357
2016-Apr-07 09:25:54	IP / UDP / OTHER	234 B	140.	-> 140. 173	49513 -> 1357

- 惡意程式 EXE 執行後， svchost.exe 除了對外部產生連線，也會內部網路進行主機掃描， 都是針對 TCP 或 UDP port 1357 。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心



- 主機感染經過一段時間後，系統被會強制關機，判斷是駭客 C&C 主機下指令操作，重新後檢查 autoruns 開機啟動區，發現有支程式會入開機啟動區，名為 notilv.exe 也就是 svchost.exe ，其連線 IP 同為 104.202.173.64 ，可以確定此 IP 為 C&C 伺服器。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心

SHA256: 2c7c9fd09a0a783badfb42a491ccec159207ee7f65444088ba8e7c8e617ab5a5

File name: c .dll

Detection ratio: 22 / 57

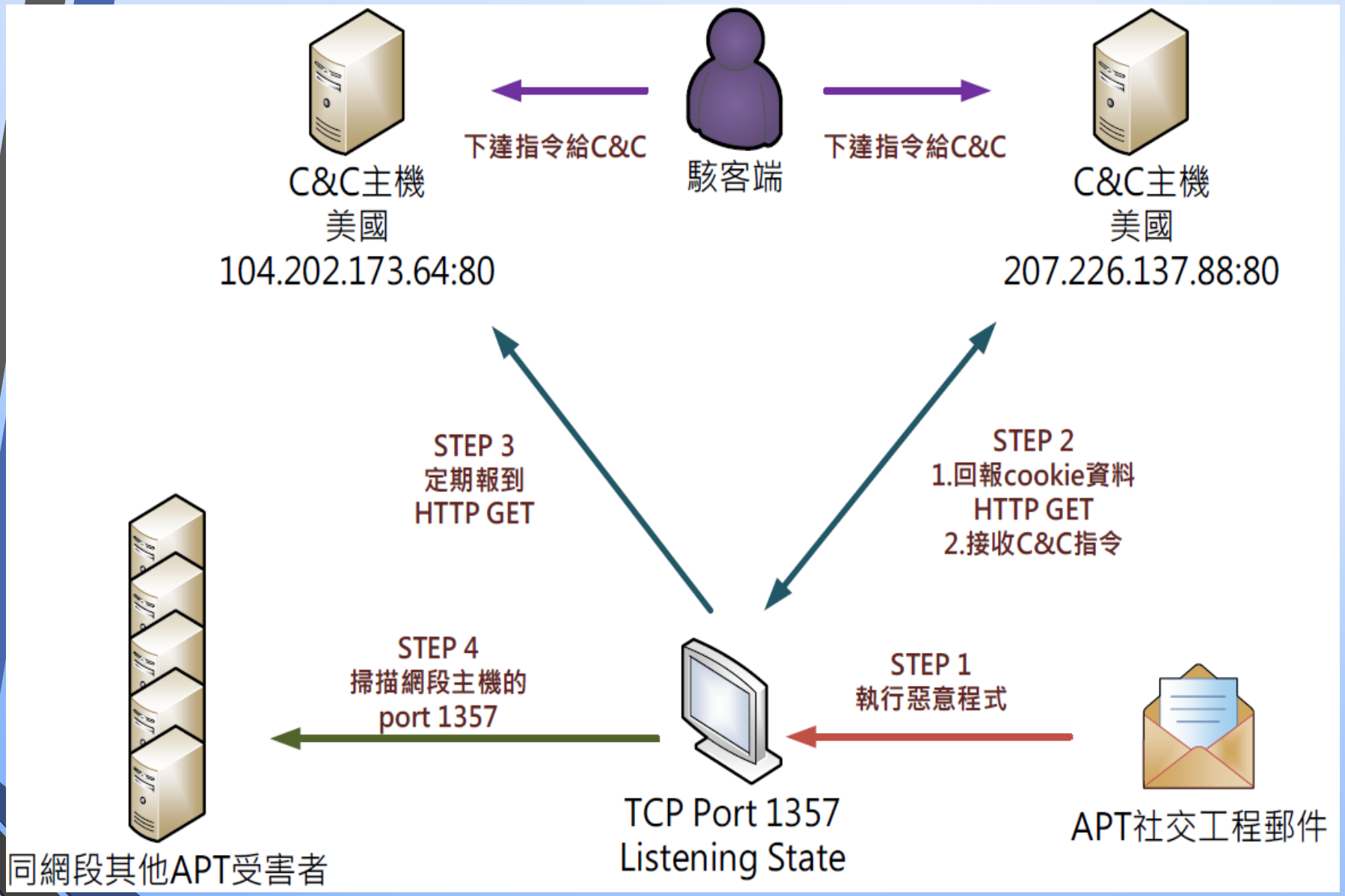
Analysis date: 2016-04-08 05:42:12 UTC (1 month ago)

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
ALYac	Trojan.GenericKD.3141527	20160408
AVware	Trojan.Win32.Generic!BT	20160408
Ad-Aware	Trojan.GenericKD.3141527	20160408
AegisLab	Bkdr.Zacom.Gen!c	20160408
AhnLab-V3	Trojan/Win32.Gen	20160407

- 透過 virustotal 掃描 notilv.exe 也就是 svchost.exe ，可以發現偵測比率為 22/57。

資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心



資料來源：社交工程郵件的APT攻擊事件分析報告，TACERT臺灣學術網路危機處理中心

社交工程郵件範例

- 包含會連到假網站連結的垃圾郵件

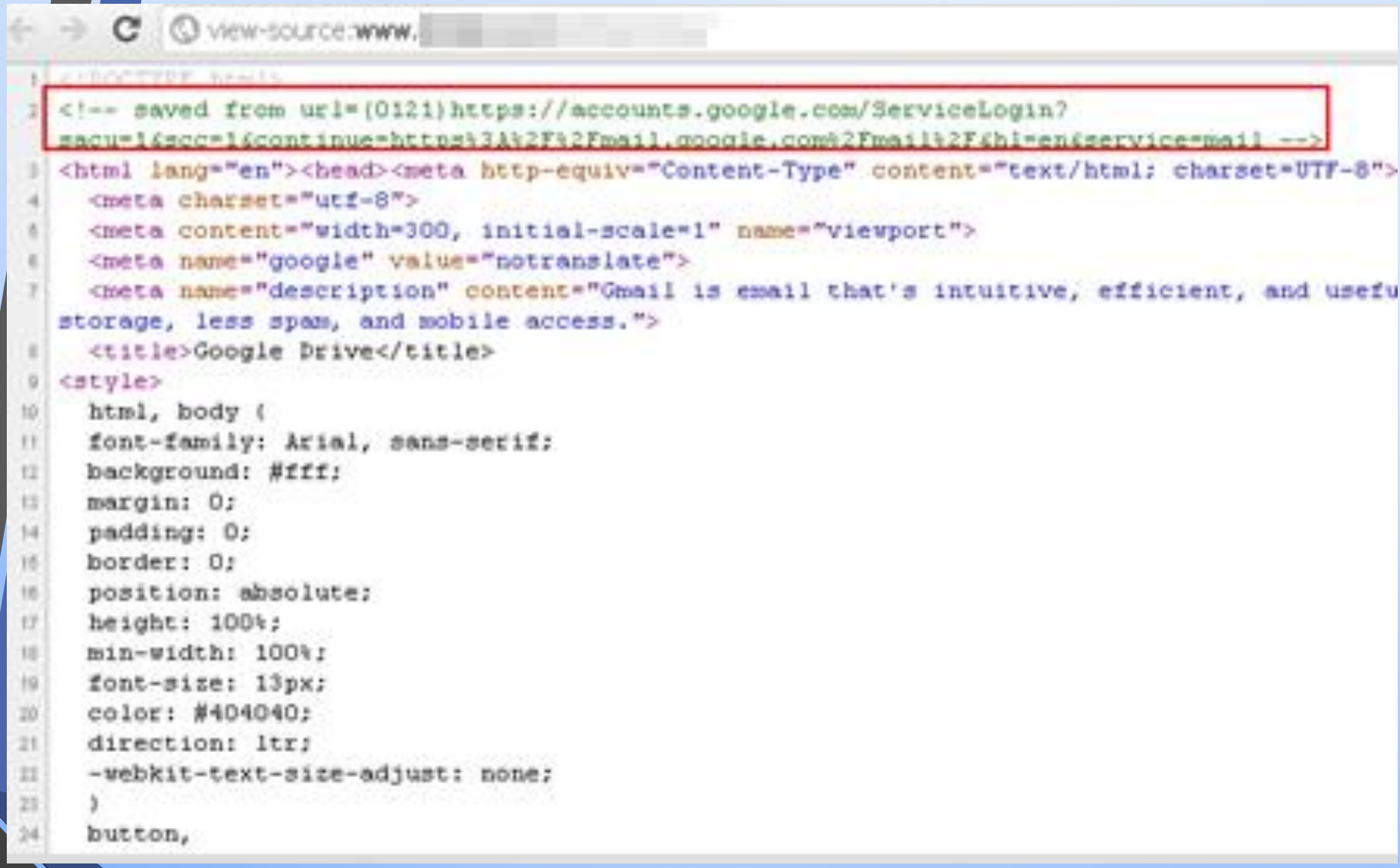
資料來源：http://blog.trendmicro.com.tw/?p=10379

◆ 假 Google Drive網站

資料來源：http://blog.trendmicro.com.tw/?p=10379

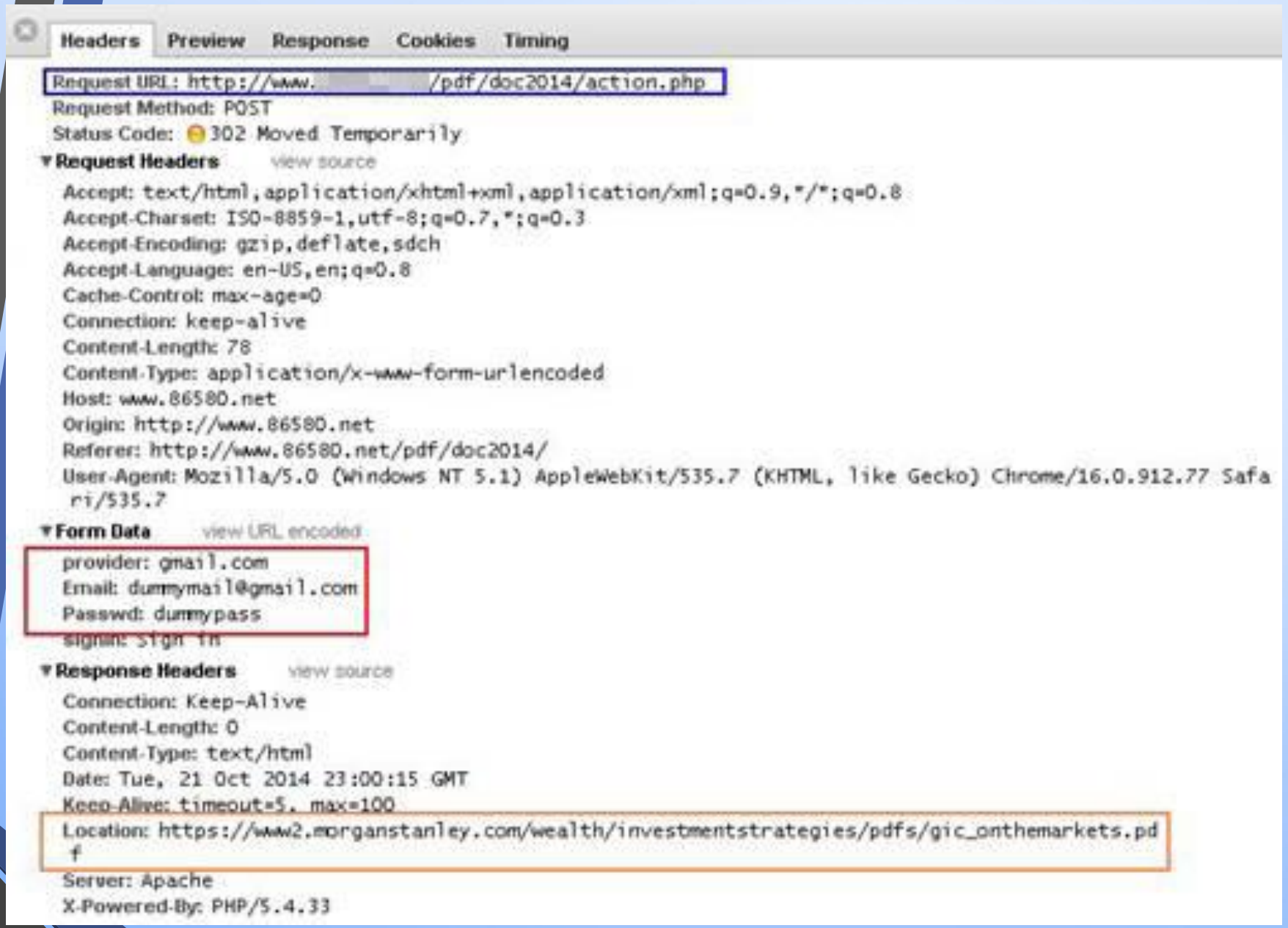
◆ 登入之後，使用者會被重新導到一合法網站

資料來源：http://blog.trendmicro.com.tw/?p=10379



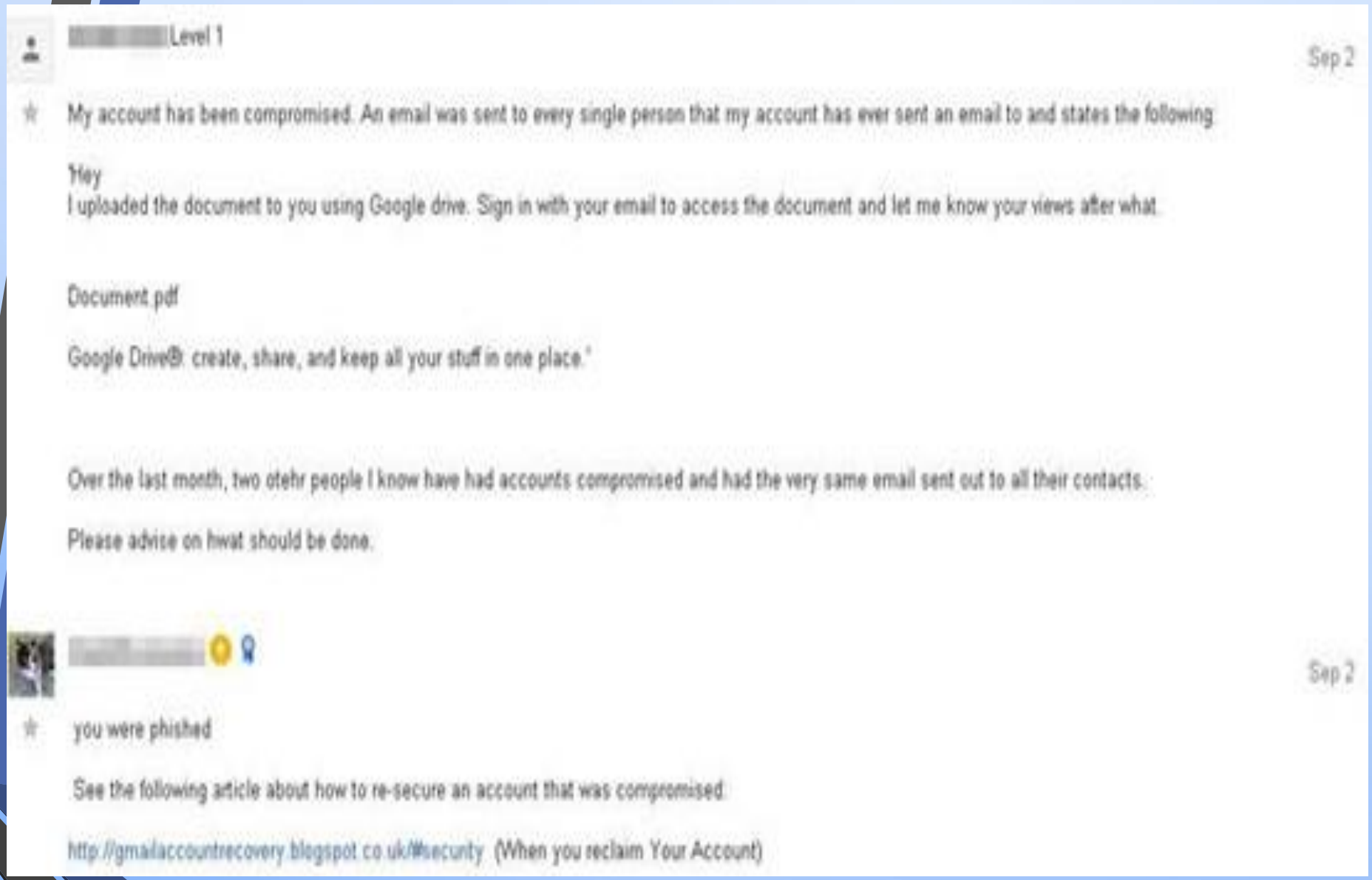
◆ 釣魚網頁程式碼顯示來自Google Drive的程式碼

資料來源：http://blog.trendmicro.com.tw/?p=10379



◆ 按下登入按鈕，認證資訊和郵件服務帳號會被送到特定網址。

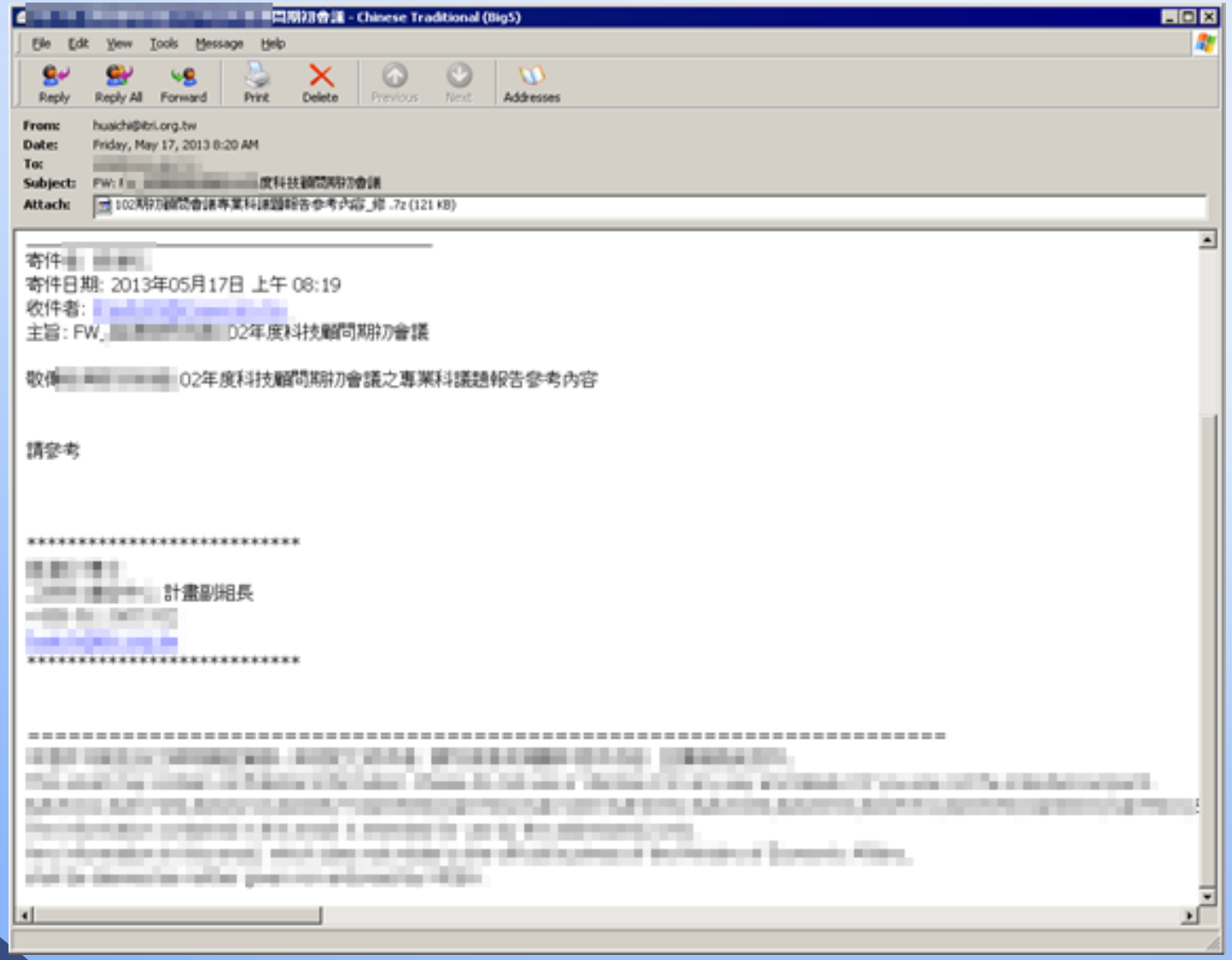
資料來源：http://blog.trendmicro.com.tw/?p=10379



◆ 網路釣魚受害者討論他們的帳號如何被用來散佈連結

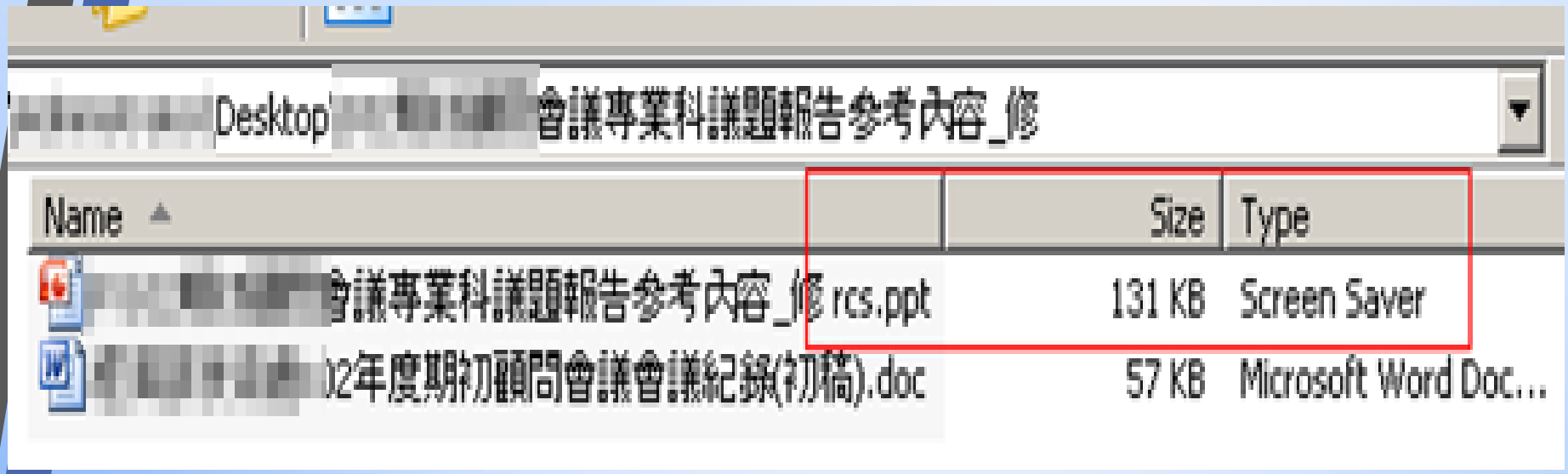
資料來源：http://blog.trendmicro.com.tw/?p=10379

社交工程郵件範例



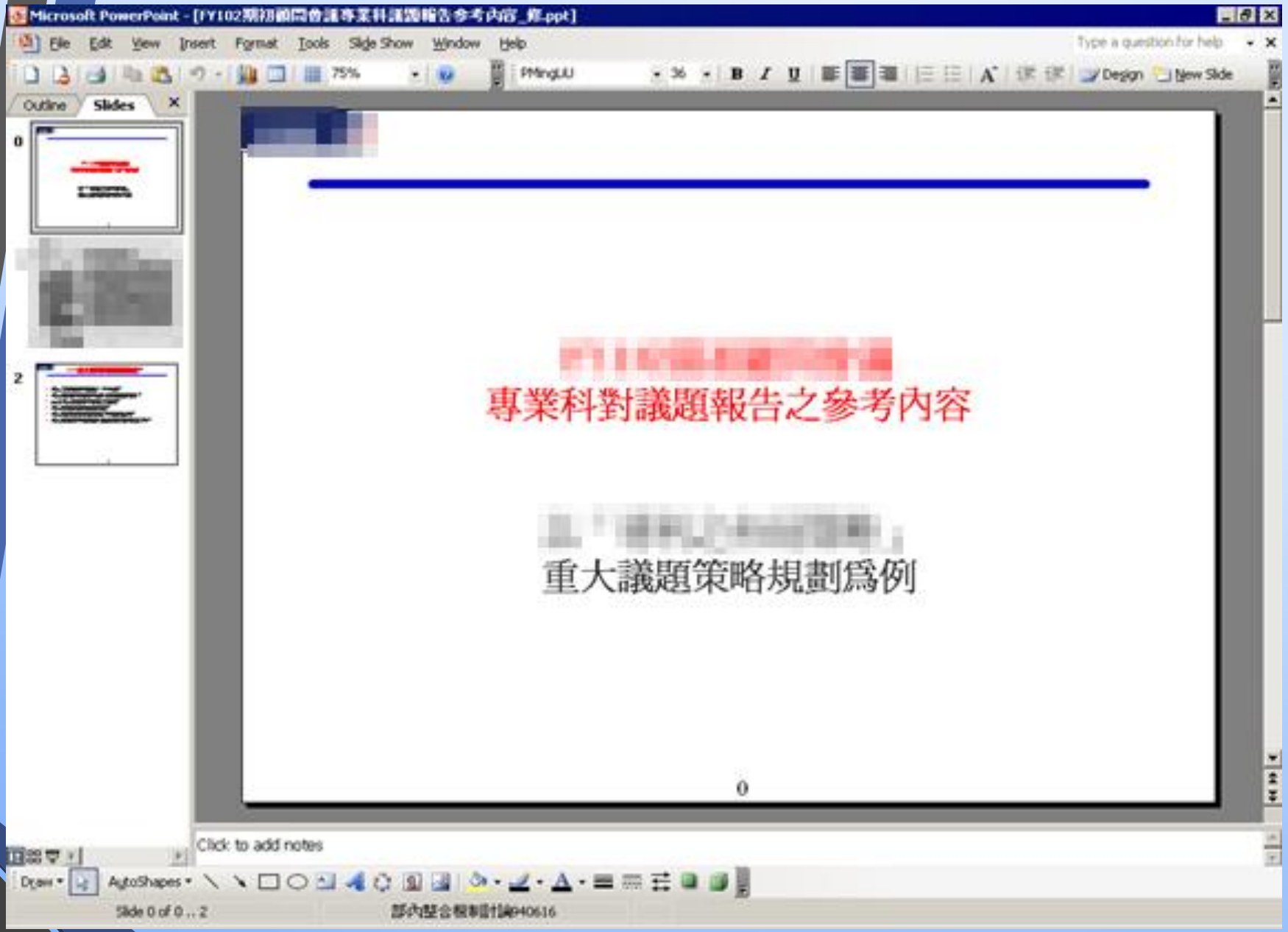
- 寄送至政府單位的電子郵件

資料來源：http://blog.trendmicro.com.tw/?p=8334



◆ 解開的附件檔顯示RTLO伎倆作用在.SCR檔案上

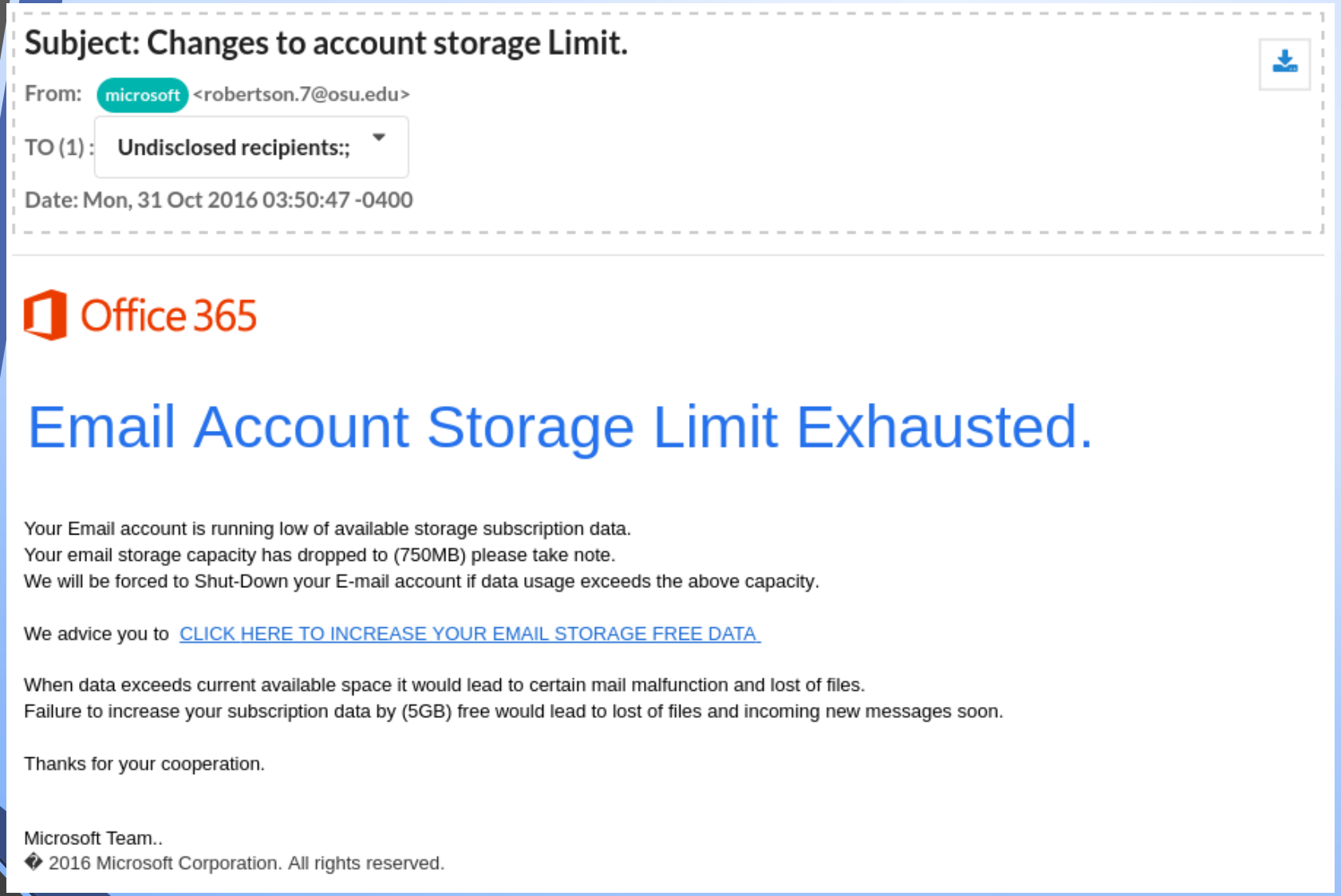
資料來源：http://blog.trendmicro.com.tw/?p=8334



◆ .SCR產生這個PPT檔案作為誘餌

資料來源：http://blog.trendmicro.com.tw/?p=8334

社交工程郵件範例



Subject: Changes to account storage Limit.

From: microsoft <robertson.7@osu.edu>

TO (1) : Undisclosed recipients:;

Date: Mon, 31 Oct 2016 03:50:47 -0400

Office 365

Email Account Storage Limit Exhausted.

Your Email account is running low of available storage subscription data.
Your email storage capacity has dropped to (750MB) please take note.
We will be forced to Shut-Down your E-mail account if data usage exceeds the above capacity.

We advice you to CLICK HERE TO INCREASE YOUR EMAIL STORAGE FREE DATA

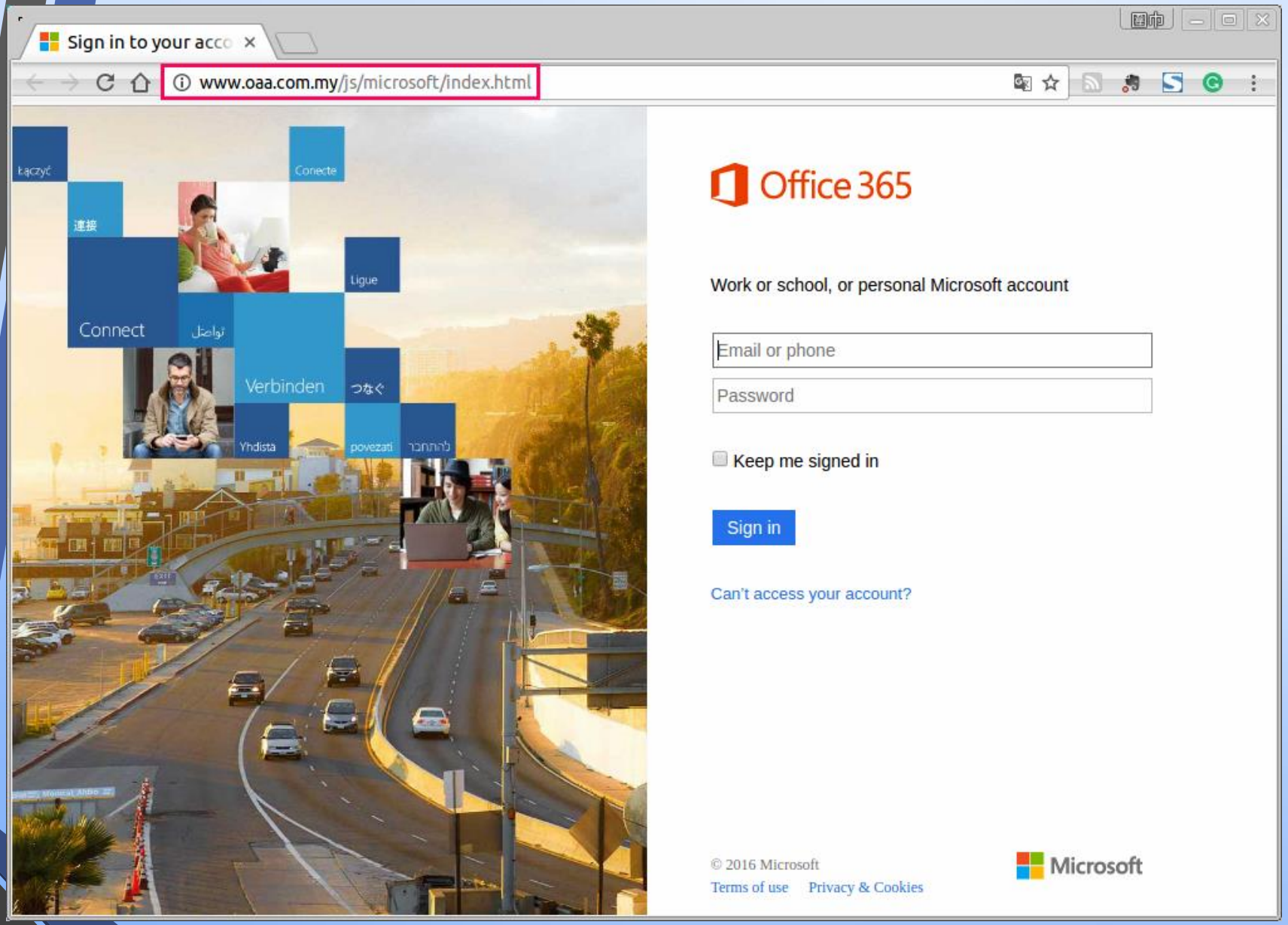
When data exceeds current available space it would lead to certain mail malfunction and lost of files.
Failure to increase your subscription data by (5GB) free would lead to lost of files and incoming new messages soon.

Thanks for your cooperation.

Microsoft Team..

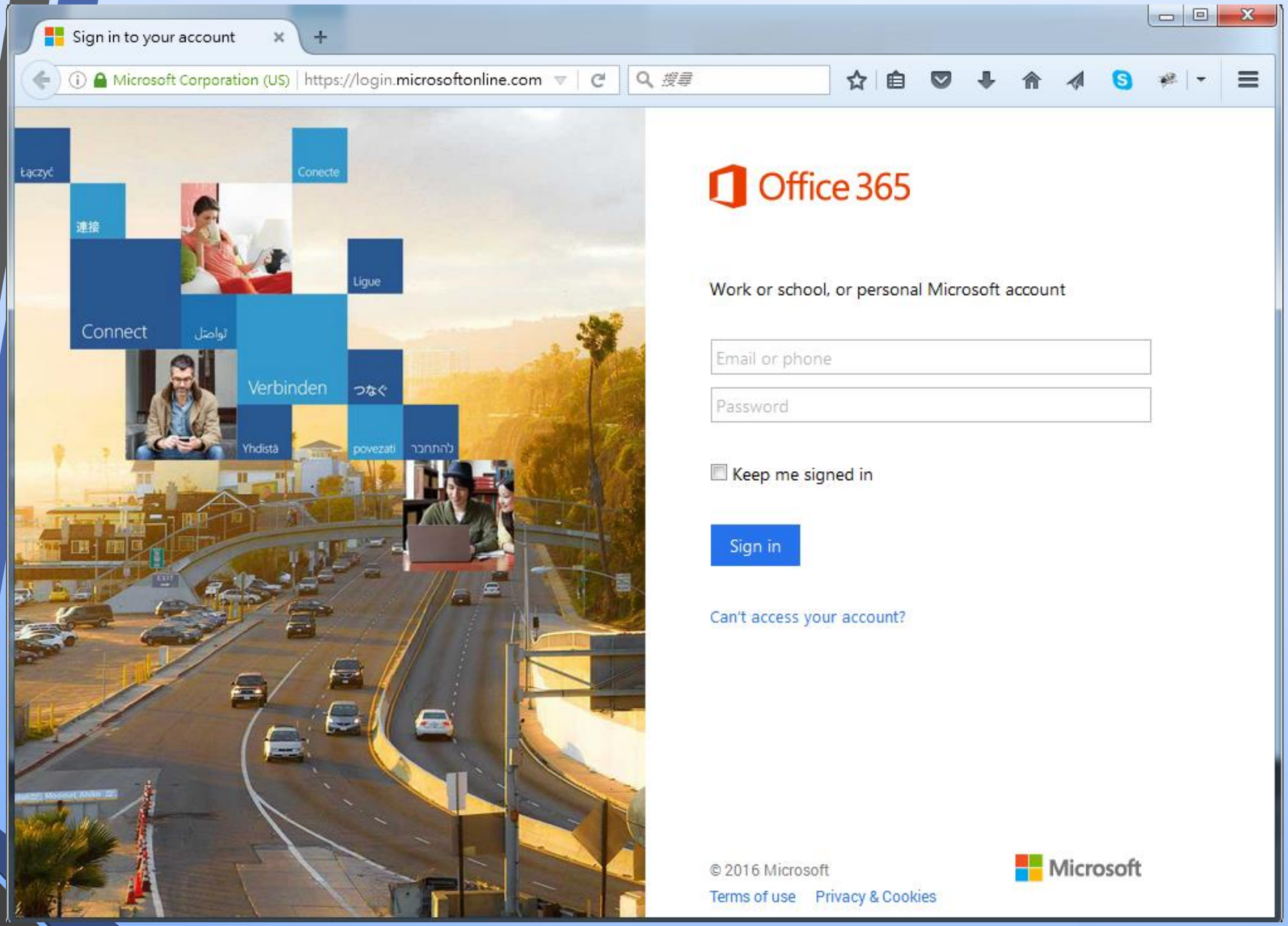
◆ 假冒 Office365 的釣魚郵件

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



◆ 點選CLICK HERE TO INCREASE YOUR EMAIL STORAGE FREE DATA 後會顯示如上圖的網頁畫面，在網址列就可以看出異樣了！

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



◆ 輸入帳密後緊接著會跳轉到正常的登入頁面。

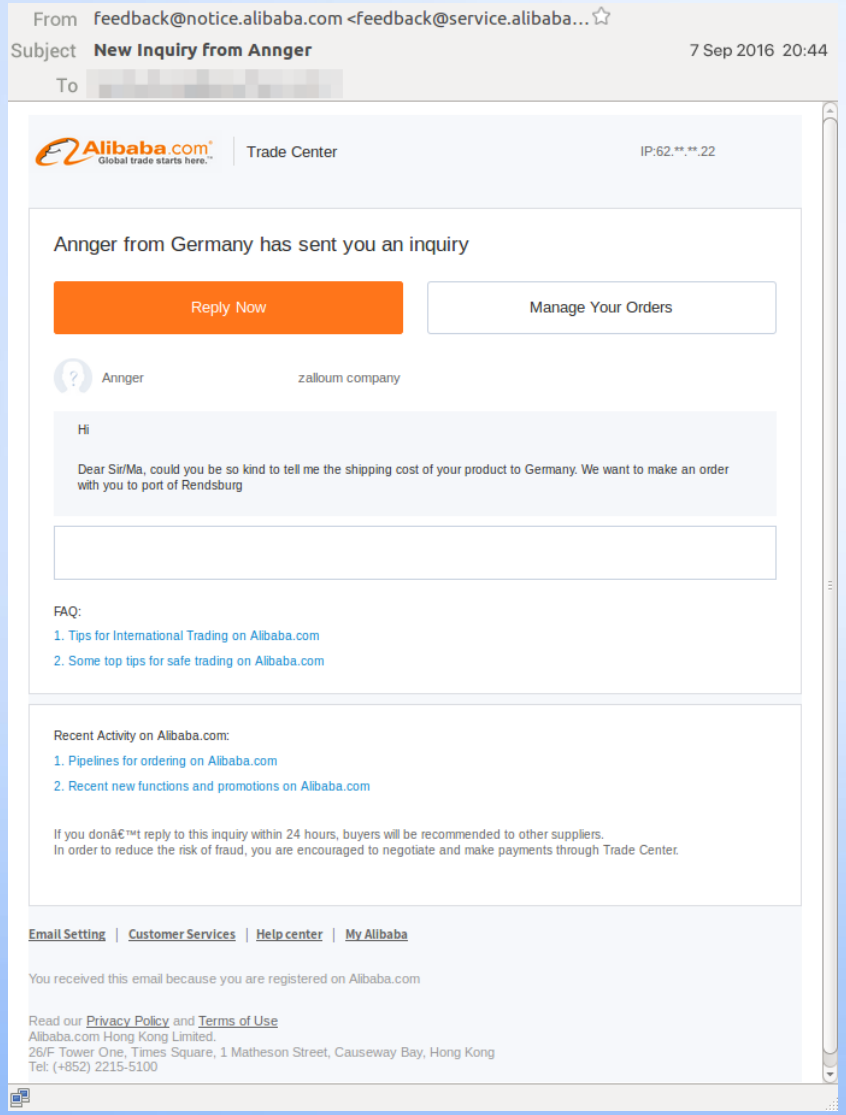
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

```
Received: from nam03-co1-obe.outbound.protection.outlook.com [(104.47.40.216)] by
        (envelope-from <robertso@math.ohio-state.edu>)
        (Cellopoint E-mail Firewall v4.1.2 Build 0314 with TLS)
        with ESMTP id 1790605569; Mon, 31 Oct 2016 16:05:17 +0800
```

- 郵件由上圖的E-mail Header/Received可看出寄件者ip雖然來自於美國微軟公司，但是envelope-from卻是@math.ohio-state.edu。

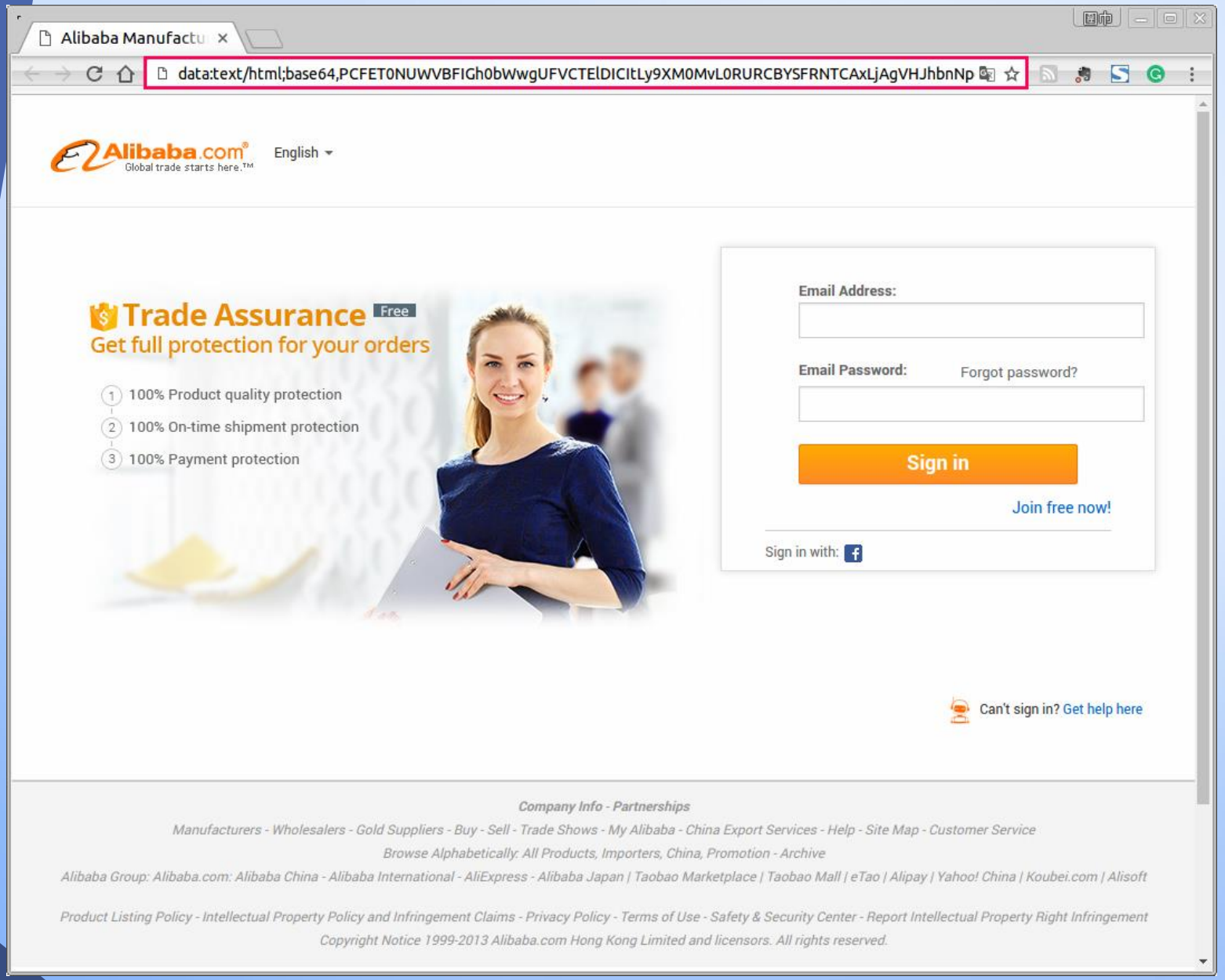
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

社交工程郵件範例



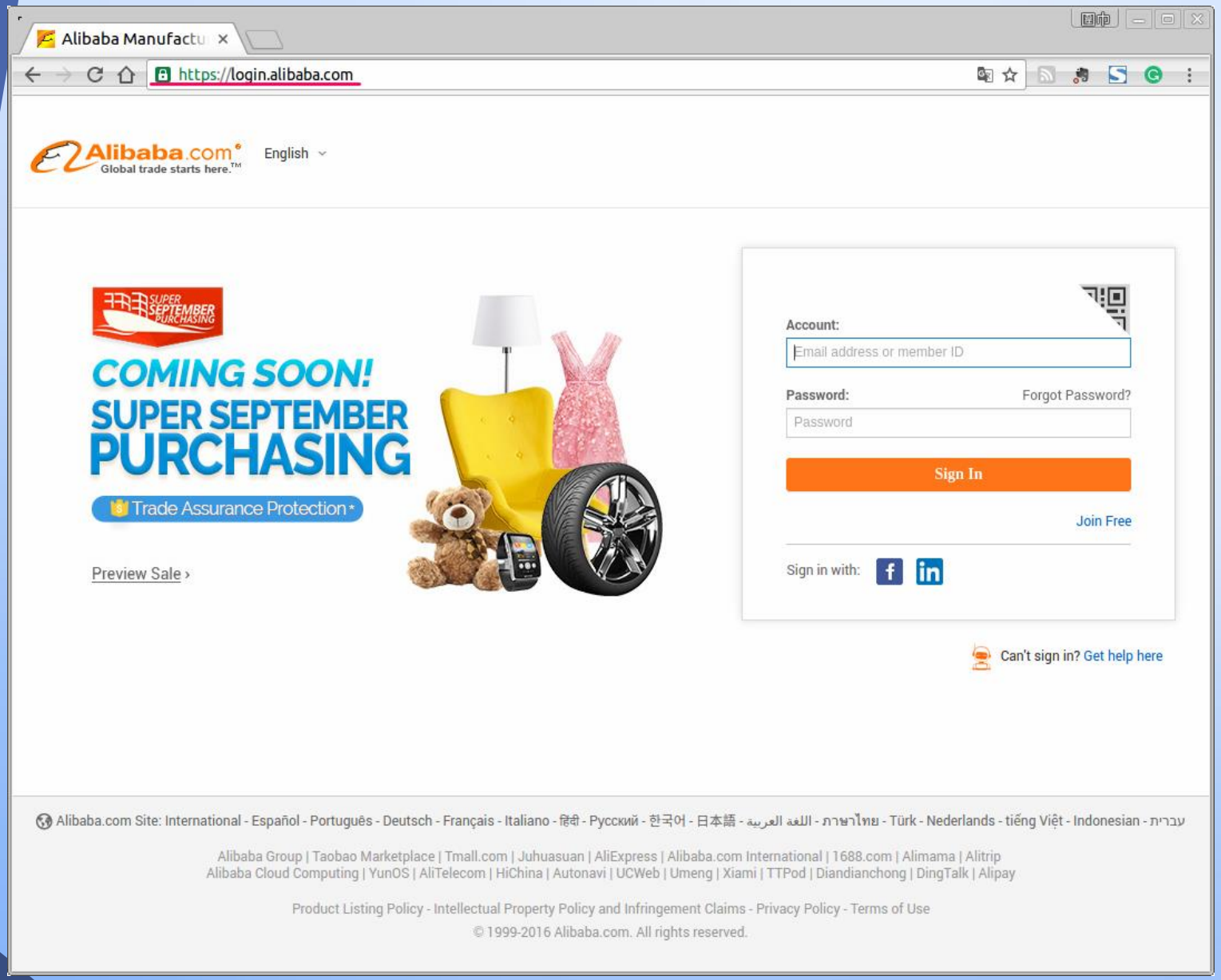
- 偽造成Alibaba的訂單需求通知。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



◆ 點選Reply now後，會進到phishing頁面

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



◆ 輸入完電子郵件及密碼後，會轉到正常的Alibaba 登錄網頁

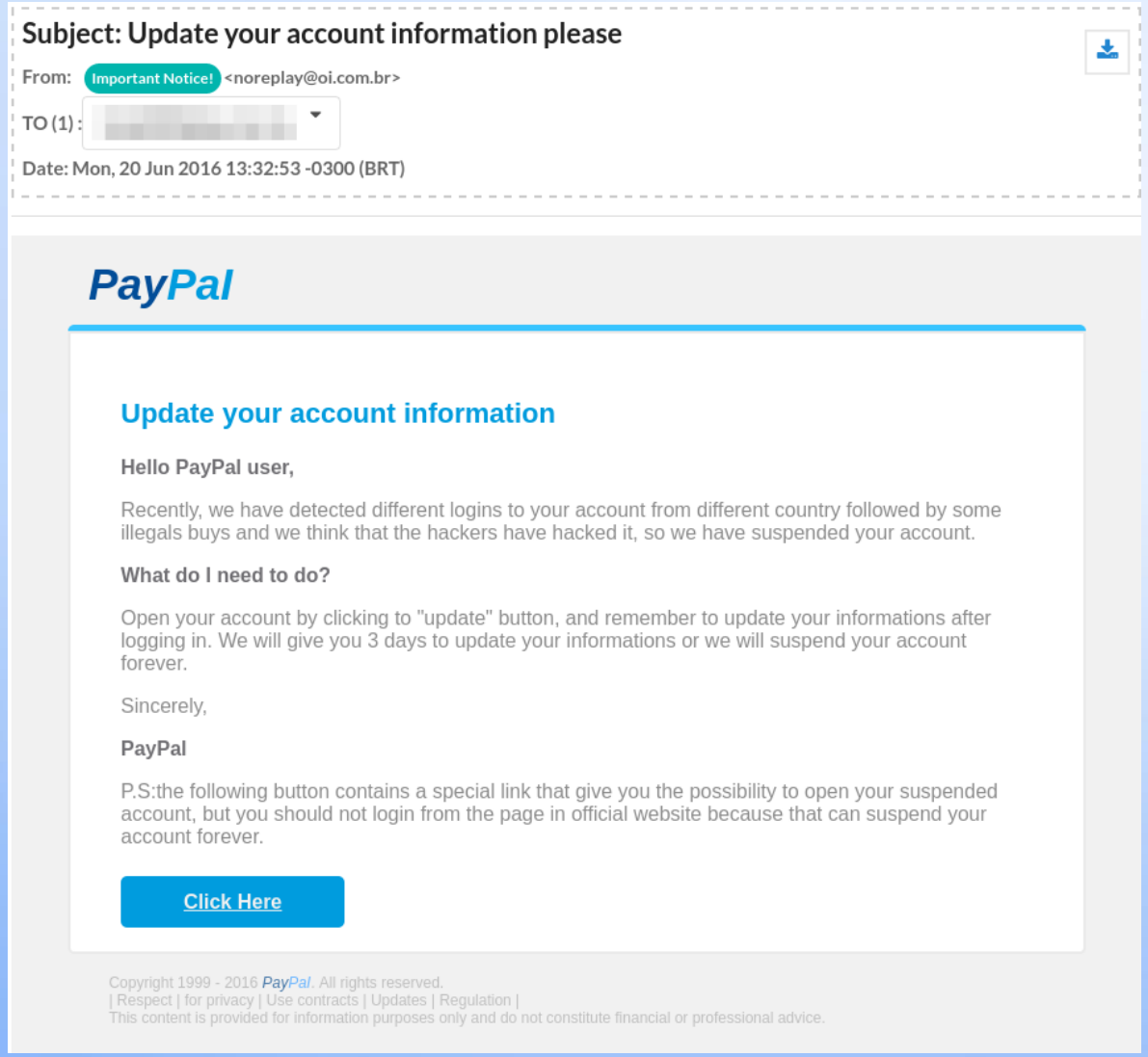
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

```
Received: from server.dnsfreedom.net [(46.166.179.209)] by
        (envelope-from <nusratlo@server.dnsfreedom.net>)
        (HQmailCello1 with TLS)
        with ESMTP id 837152110; Wed, 07 Sep 2016 20:44:09 +0800
Received: from nusratlo by server.dnsfreedom.net with local (Exim 4.87)
        (envelope-from <nusratlo@server.dnsfreedom.net>)
        id 1bhcCz-0041j6-Hc
        for Sandy.Deng@pouchen.com; Wed, 07 Sep 2016 14:44:05 +0200
To: Sandy.Deng@pouchen.com
Subject: New Inquiry from Annger
X-PHP-Script: nusratloves.com/zorobo.php for 160.152.41.141, 212.129.55.2
MIME-Version: 1.0
Content-type: text/html; charset=iso-8859-1
From: feedback@notice.alibaba.com <feedback@service.alibaba.com>
```

- 此郵件寄件者來自於紐西蘭，spammer也一併將郵件中Header/Received裡的From改成feedback@notice.alibaba.com，以取信於user。

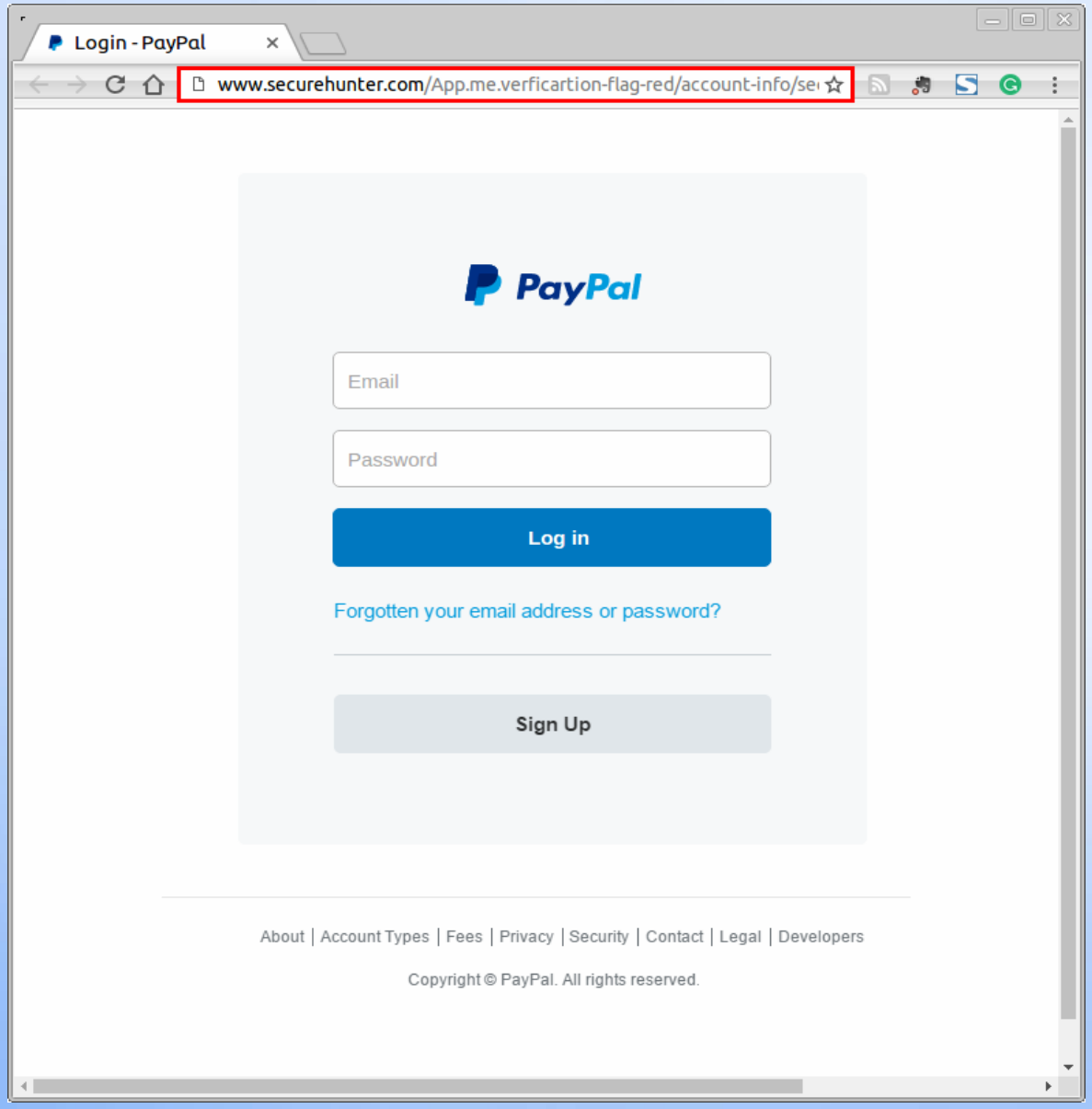
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

社交工程郵件範例



◆ 偽冒PayPal通知。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



- 點擊“更新”按鈕後會開啟轉址後的釣魚頁面，由網址列就可以很容易的看出這是個釣魚網頁。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

社交工程郵件範例

Subject: 電子郵件 地址 驗證 信息

From: Hinet网络邮件 <jordikingbikes@gmail.com>

TO (1) : undisclosed-recipients:;

Date: Fri, 29 Apr 2016 06:54:03 +0100

尊敬的用戶，

我們檢測到可疑活動在您的帳戶被病毒發送到我們的服務器系統。這可能造成的文件最近被您下載 **星期五，2016年4` 月25日下午12:02 GMT.**

你需要驗證您的帳戶，以保持發送和接收郵件，如果不是你的電子郵件將在24小時內被封鎖。

請 按照 下面 的 鏈接, 讓 您 的 賬戶 安全

點擊 驗證

中華電信數據通信分公司地址：台北市信義路一段21號全區24小時免費服務電話：0800- 080-412

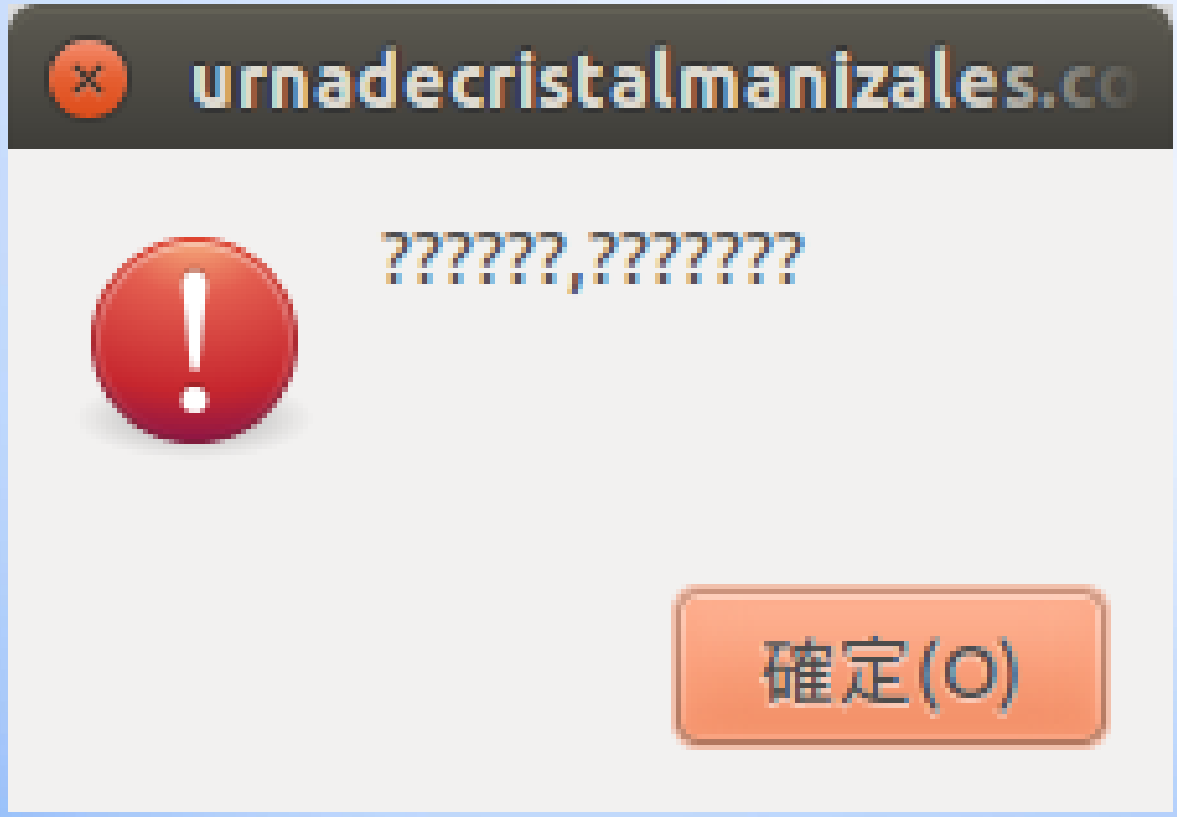
© 版權所有 2016 年 中華 電信 的 互聯網 服務 由 中華 電信.

- 由內容文字可以看到語意不明，顯然是透過翻譯器翻譯過來的文字。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

◆ 選擇上圖「點擊驗證」按鈕會開啟如下圖的釣魚網頁。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



◆ 輸入帳號密碼按下OK後會彈出一個錯誤訊息。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

◆ 按下「確定」後畫面會緊接著連結到真正的Hinet登入頁面。

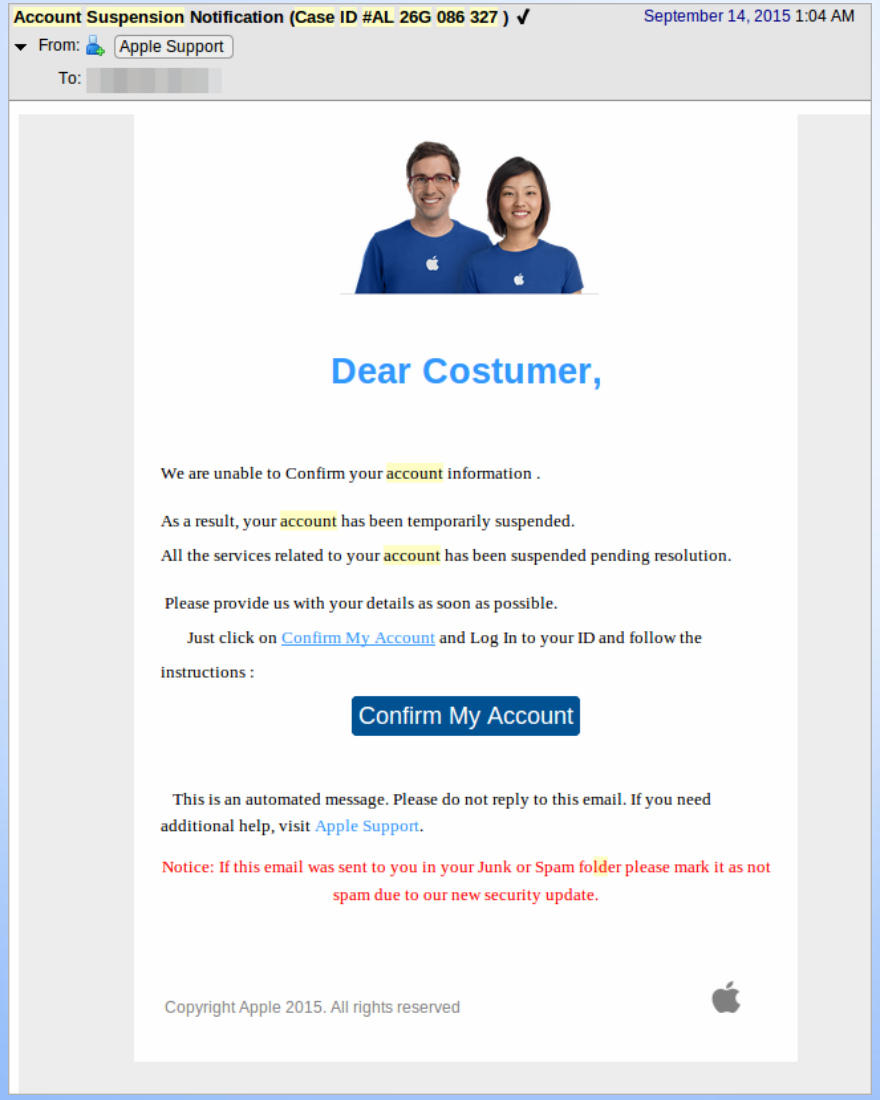
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

Received: from mail-ob0-f180.google.com [(209.85.214.180)] by [redacted]
(envelope-from <jordikingbikes@gmail.com>)
(Cellopoint E-mail Firewall v3.9.12 Build 0813 with TLS)
with ESMTP id 1001918214; Fri, 29 Apr 2016 13:54:09 +0800

- 這封信的E-mail Header/Received，可以看出spammer是使用Google的帳號寄出此信件，看來public的帳號有時也很難避免成為網路犯罪的溫床。

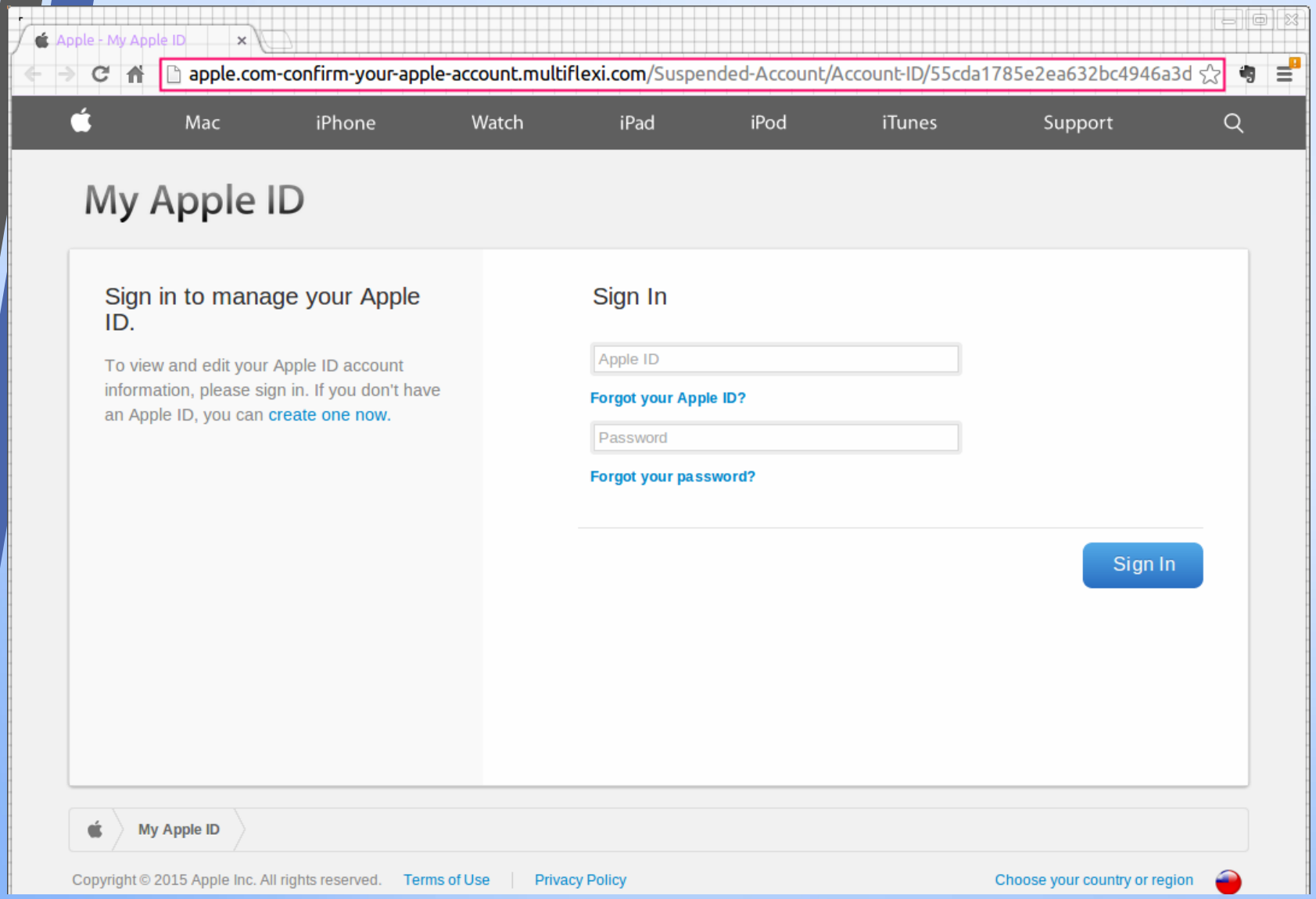
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

社交工程郵件範例



- 偽冒Apple的釣魚郵件。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19



- 點選 Confirm My Account 後會開啟釣魚網頁，網址列裡的英文字母乍看之下確實有“apple”的字眼，遇到以上情形還是請由官網登入，不隨意開啟來路不明的信件，並且持著謹慎的態度勿隨意點選信中的連結。

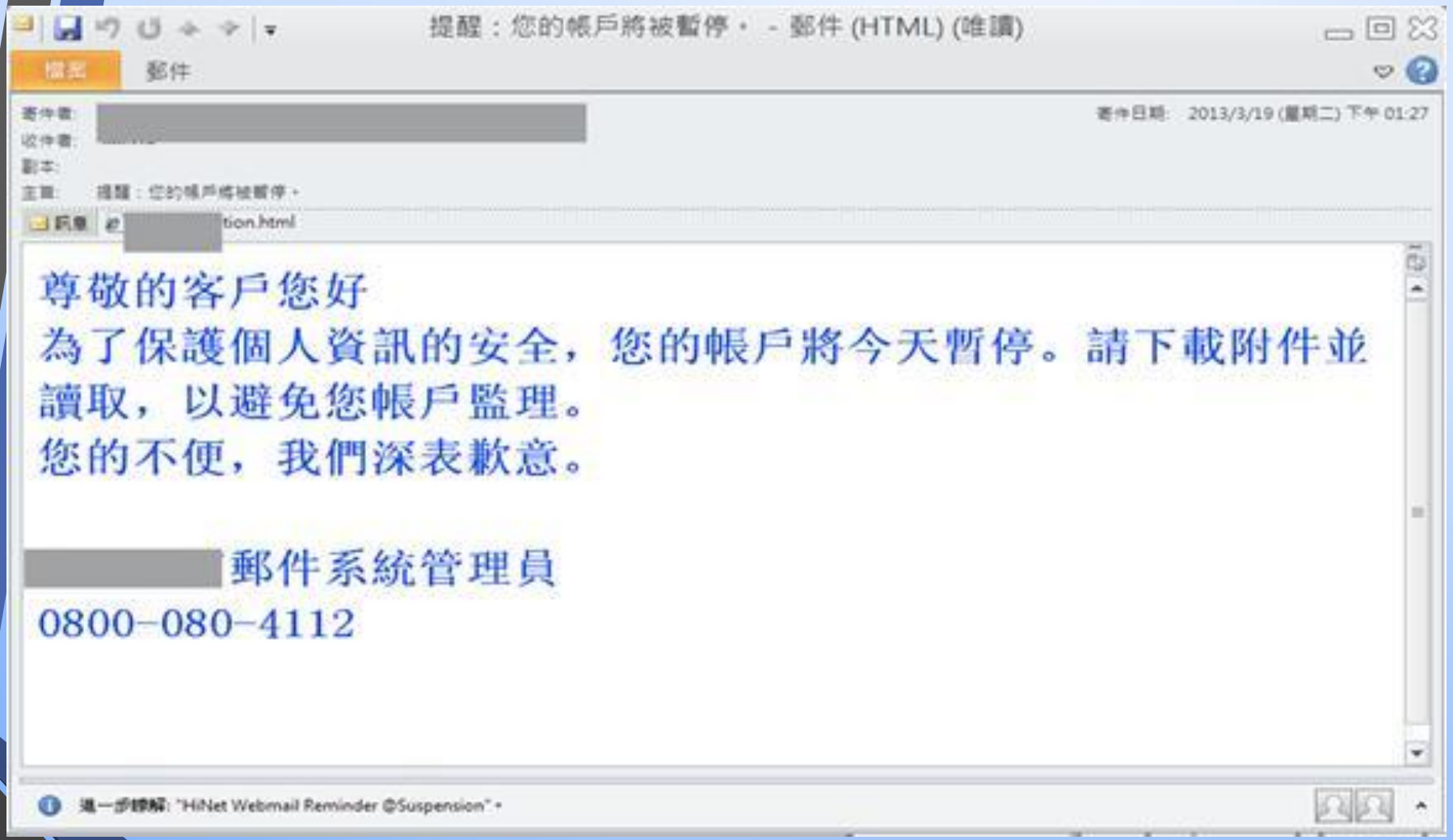
資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

Received: from mail.siteskins.net [(207.114.89.37)] by [redacted]
(envelope-from <siteskins@mail.siteskins.net>)
(s01mx.horus.it)
with ESMTP id 1656873851; Sun, 13 Sep 2015 19:39:37 +0100
Received: by mail.siteskins.net (Postfix, from userid 501)
id 2F9F23A2D16; Sun, 13 Sep 2015 13:04:56 -0400 (EDT)
Date: Sun, 13 Sep 2015 17:04:56 +0000
To: [redacted]
From: Apple Support <Apple@Support.com>

- 釣魚郵件 envelope。

資料來源：http://www.cellopoint.com/tw/taxonomy/term/19

社交工程郵件範例



- 假冒email系統管理員的郵件至特定的承辦人員信箱

資料來源：http://blog.trendmicro.com.tw/?p=32893

1. 駭客跟你一起關心熱門新聞?!

   熱門新聞被駭主旨一覽：

- 年金改革
- 106年政府行政機關辦公日曆表
- 黑心食品一覽表

資料來源：http://blog.trendmicro.com.tw/?p=32893

2. 駭客比你同事還了解你?!
鎖定個人被駭主旨一覽：

- ○○會議名單更新
- 員工滿意度調查(寄件人:求職者)
- 求職信(寄件人:應徵者)
- 你的帳號即將關閉(寄件人:email系統管理員)
- 請儘速到我辦公室(寄件人:老闆)
- 電信帳單(寄件人:某知名電信公司)
- 銀行交易明細(寄件人:某銀行)
- 假冒email系統管理員的郵件至特定的承辦人員信箱表

資料來源：http://blog.trendmicro.com.tw/?p=32893

3. 勒索軟體曾經使用過的網路釣魚主旨或手法：

- 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
- iPhone中獎通知
- 求職信
- 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）

資料來源：http://blog.trendmicro.com.tw/?p=32893

防止社交工程信件上鉤7步驟

- 點選連結前,先移動滑鼠檢查真實來源。
- 勿回覆要求提供個人資料的電子郵件-即使信中有該公司的商標。
- 不要向不請自來的電訪人員透露任何個人或同事資料。
- 避免開啟網路上之任何附件檔，可利用網路安全軟體先行掃過後再開啟。
- 直接在瀏覽器輸入網址或是將常用網站加到我的最愛/書籤清單中。
- 搜尋網頁，請確認網址真實性，避免以假亂真,比如英文O變造為數字0;字母l 變造為數字 1。
- 定期更新瀏覽器漏洞，並更新至最新版本。

資料來源：http://blog.trendmicro.com.tw/?p=32893

釣魚網站

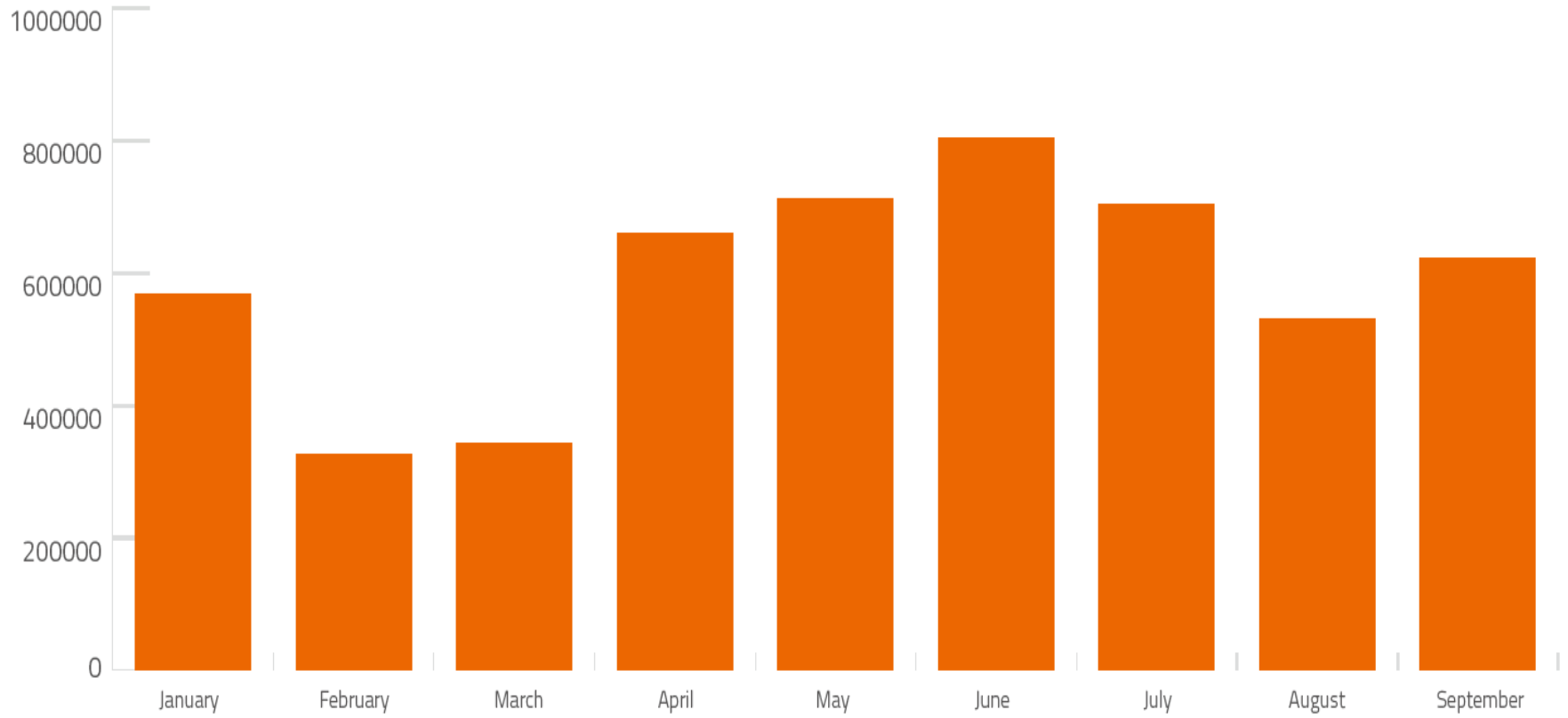


Figure 1: Phishing Sites by Month, 2016 Q1-Q3

資料來源：Webroot Phishing Threat Trends，Weproot

8成釣魚網站快閃詐騙

84% of phishing sites last less than 24 hours.

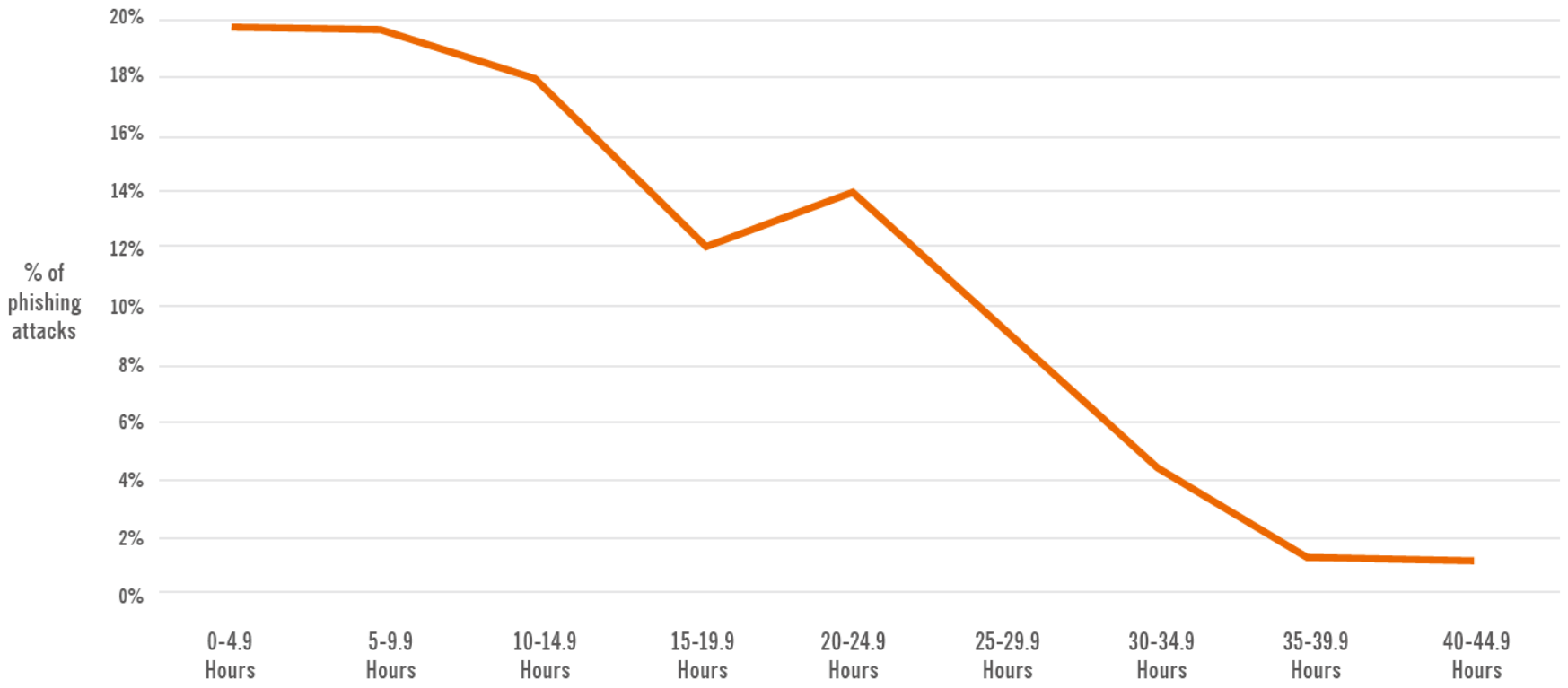


Figure 2: Phishing Attack Life Cycles in Hours

資料來源：Webroot Phishing Threat Trends，Weproot

釣魚網站模擬正式網站

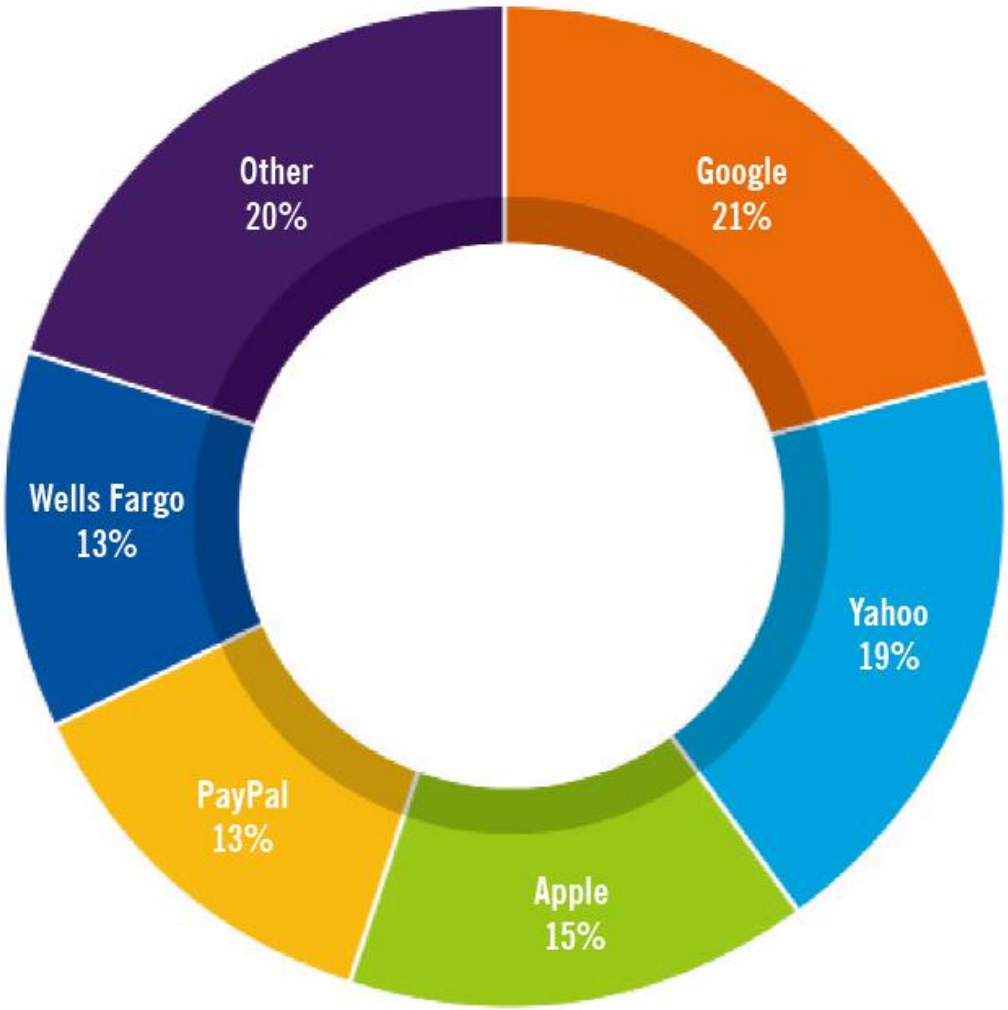


Figure 4: Relative Share of Phishing Sites for Highest-Risk Companies

資料來源：Webroot Phishing Threat Trends，Weproot

釣魚網站模擬正式網站趨勢

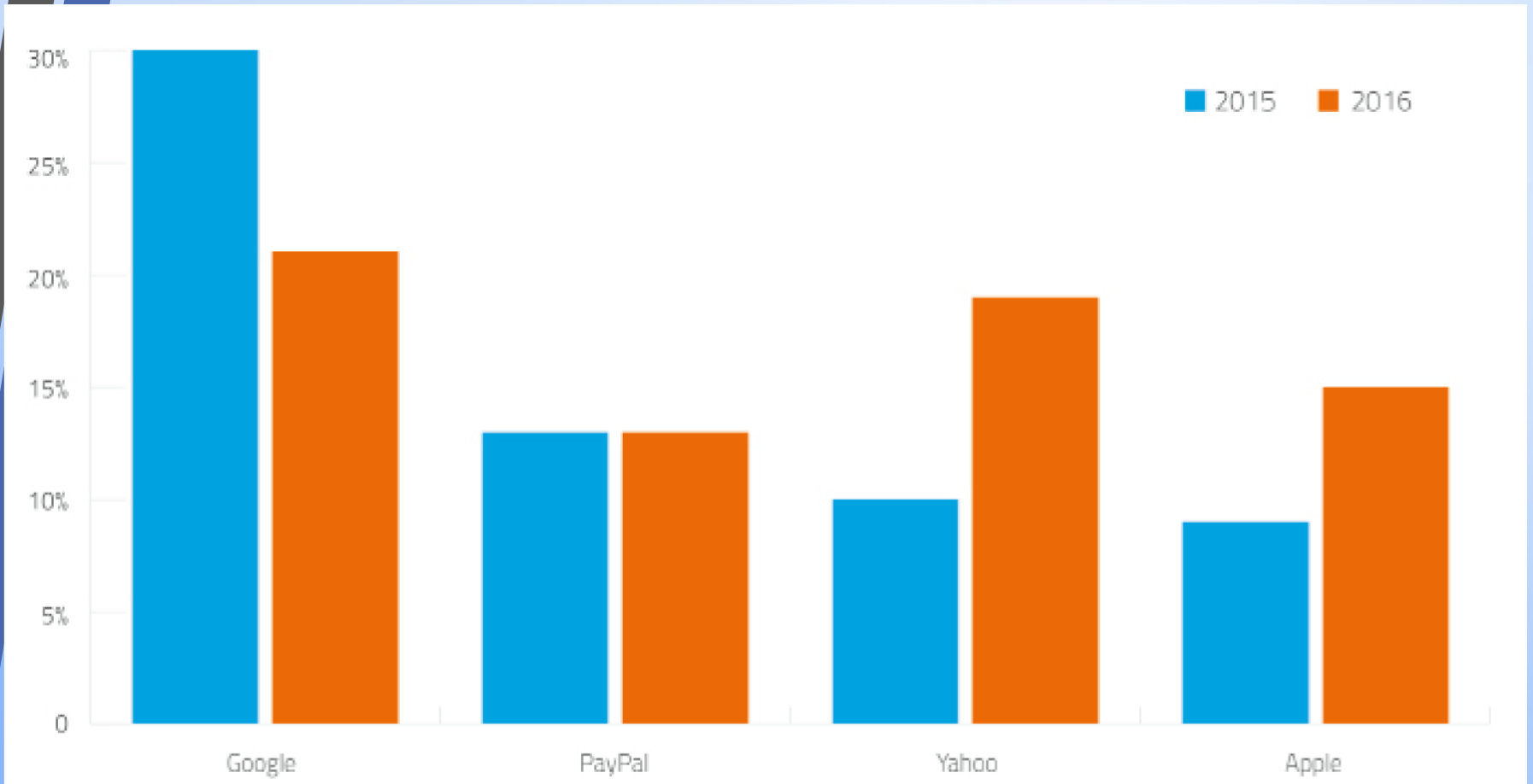


Figure 5: Share of Phishing Sites for Highest-Risk Companies in 2015 and 2016

資料來源：Webroot Phishing Threat Trends，Weproot

釣魚網站範例

資料來源：http://www.pcdiy.com.tw/detail/1869

2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

四個問題 問題二:

您對 Chrome 之前版本的滿意度?

- ◉ 非常滿意
- ○ 比較滿意
- ○ 一般
- ○ 非常不滿意

下一個...

資料來源：http://www.pcdiy.com.tw/detail/1869

2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

四個問題 問題三.

您使用的其他流覽器是哪一款?

- ◉ 只使用 Chrome
- ○ Internet Explorer
- ○ Firefox
- ○ 其他

下一個...

資料來源：http://www.pcdiy.com.tw/detail/1869

資料來源：http://www.pcdiy.com.tw/detail/1869

資料來源：http://www.pcdiy.com.tw/detail/1869

2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

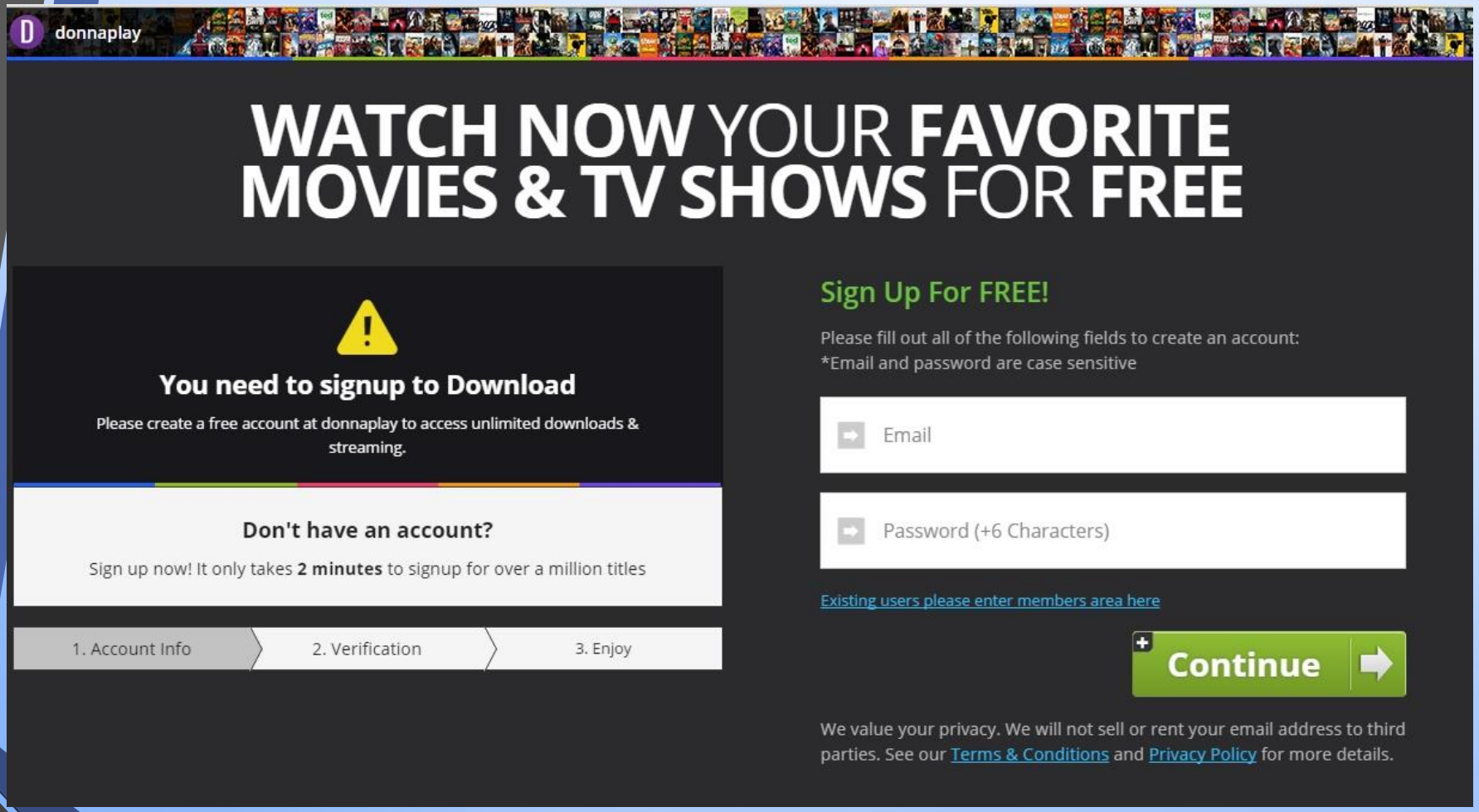
感謝您完成此次調查！為感謝您的參與，我們提供了以下幾項選擇：**Thursday, June 25, 2015.**
請選擇 (**僅限今天**):

HD Streaming Movies

正常價格: ~~NT$ 2300~~
僅限今天: **NT$ 0.00**

剩餘數量: 1 點擊這裡 →

資料來源：http://www.pcdiy.com.tw/detail/1869



資料來源：http://www.pcdiy.com.tw/detail/1869

社群 統計資料 文件 常見問題集 關於 繁體中文 加入我們的社群 登入

virustotal

URL: https://www.donnaplay.com/signup?ad_domain=ads.ad-center.com&ad_path=%2Fsmart_ad%2Fdisplay&prod=21&ref=5033402&spid=KN10GQXUBo&seed=2795297080&sf=eone&adserver=0.16.0&m=movies&skin=night

偵測率: 2 / 63

分析日期: 2015-06-25 07:12:47 UTC (0 分鐘 前)

分析 其他資訊 評論 投票

網址掃瞄器	結果
Avira	Malware site
BitDefender	Malware site
ADMINUSLabs	Clean site

資料來源：http://www.pcdiy.com.tw/detail/1869

釣魚網站範例

- 「真」iCloud 網站 http://www.icloud.com

資料來源：https://mrmad.com.tw/note-apple-users-please-be-careful-icloud-fishing-websites

◆ 「假」iCloud 網站 http://www.apple-icloud.com

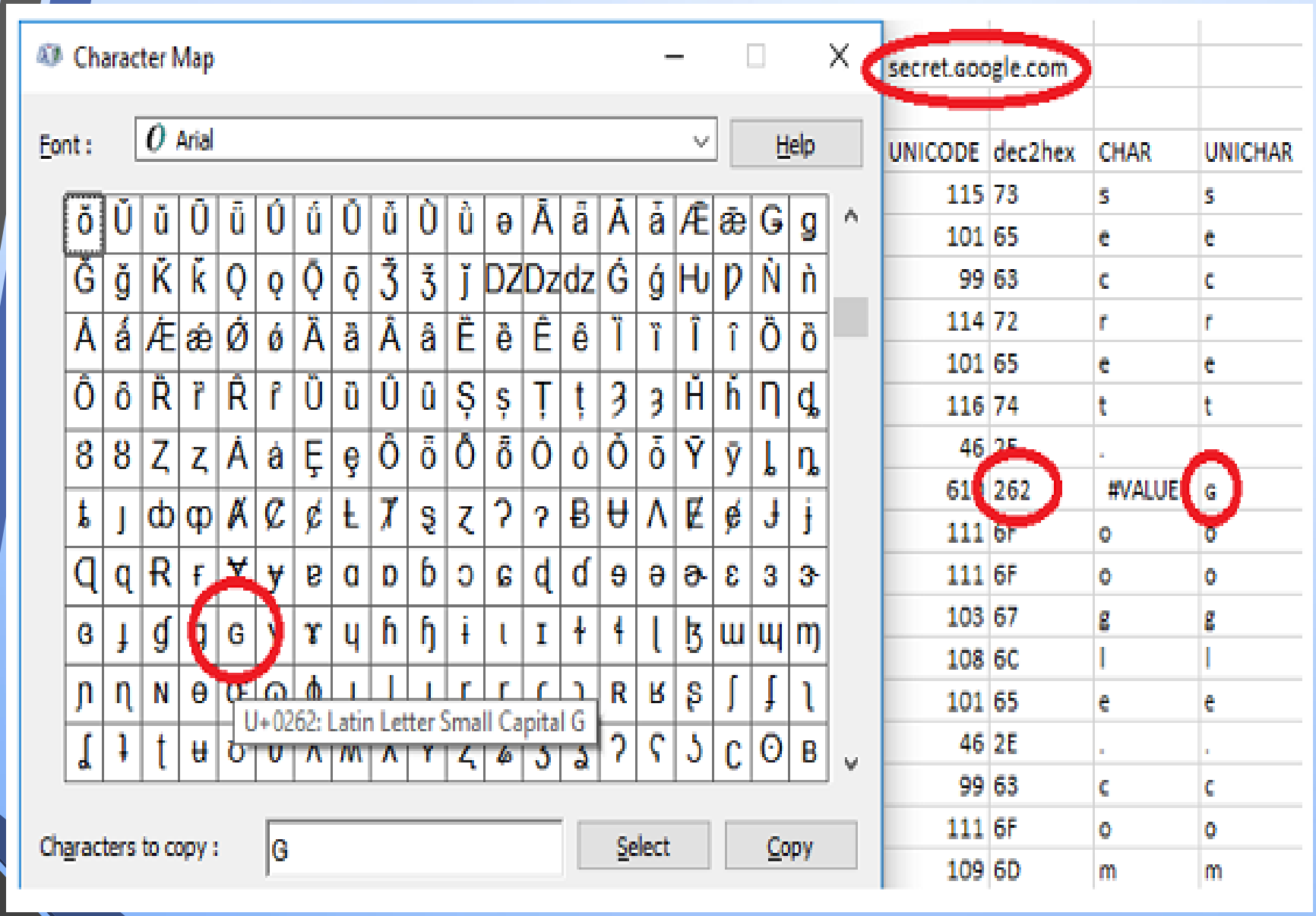
資料來源：https://mrmad.com.tw/note-apple-users-please-be-careful-icloud-fishing-websites

資料來源：https://mrmad.com.tw/note-apple-users-please-be-careful-icloud-fishing-websites

釣魚網站範例

Google.com

Google.com



資料來源：http://technews.tw/2016/11/23/watch-%C9%A2ooglecom-is-not-googlecom/

virustotal

URL:	http://xn--oogle-wmc.com/
偵測率:	6 / 68
分析日期:	2016-12-22 06:39:27 UTC (0 分鐘 前)

分析 | 其他資訊 | 評論 | 投票

網址掃瞄器	結果
Certly	Malicious site
CLEAN MX	Malicious site
Sophos	Malicious site
Fortinet	Malware site
BitDefender	Phishing site

lifehacker

lifehacker

URL: http://xn--lifehacer-1rb.com/

偵測率: 0 / 68

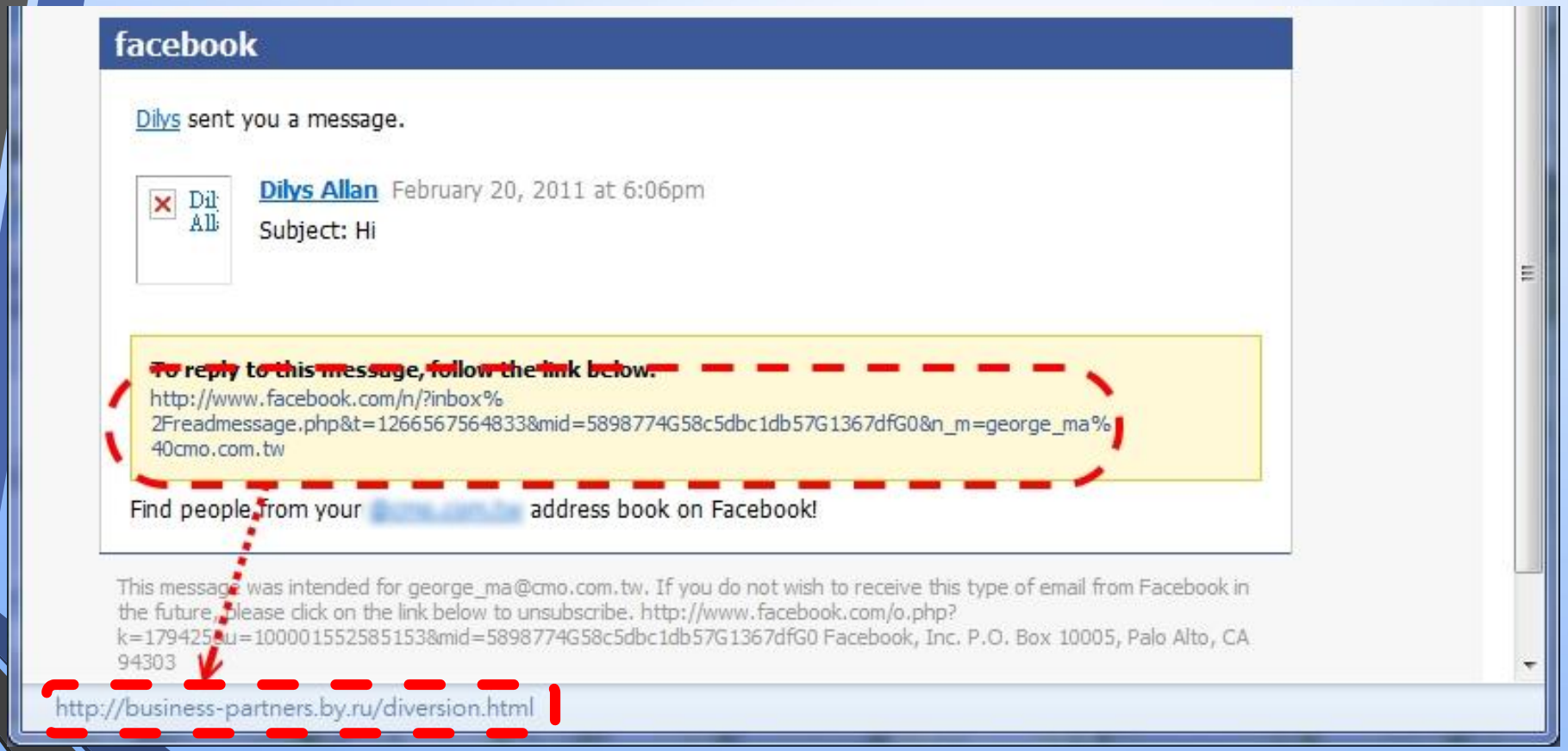
分析日期: 2016-12-22 06:38:26 UTC (6 分鐘 前)

分析 | 其他資訊 | 評論 0 | 投票

網址掃瞄器	結果
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira (no cloud)	Clean site
Baidu-International	Clean site

分辨釣魚網址

- 顯示位址與連網位址相異



資料來源：http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6813

- 網址混淆
  - http://mail-google.com
  - http://www.goog1e.com
  - http://mail.google.com.xyznothisdomain.com
- 網站轉址
  - http://rd.yahoo.co.jp/*http://www.isecutech.com.tw/
- 縮址服務
  - http://goo.gl/8GRT

資料來源：http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=6813

簡報大綱

- 個資暨資安案例分享
- 2017年資安預測
- 釣魚郵件與網站介紹與防護
- 物聯網(IoT)資安
- 勒索軟體介紹與防護

傳輸技術大躍進，物聯網市場今年挑戰破兆

- 市調機構IDC預測，2017年全球IoT市場規模將超過9 ,300億美元，較去年多增加1千億，今年有機會挑戰破兆。3年後，預計市場將達到應用爆發期，規模更將翻倍成長達1.46兆美元。
- 全球IoT裝置數量成長更快速，5年內將翻漲3倍， 2015年全球IoT裝置數量已有121億個，明年將超越手機，未來3年，全球IoT裝置總數將累積高達300億個。。

資料來源：http://www.ithome.com.tw/news/111022

IOT-個人

手機

平板

筆電

電腦

數位相機

智慧手環

智慧手錶

遠端醫療

IOT-家庭

ADSL數據機

無線分享器

網路監視器

網路印表機

網路儲存設備

保全系統

智能管家

智能家電(電視、冰箱、冷氣、咖啡機、電燈、洗衣機、門鎖...)

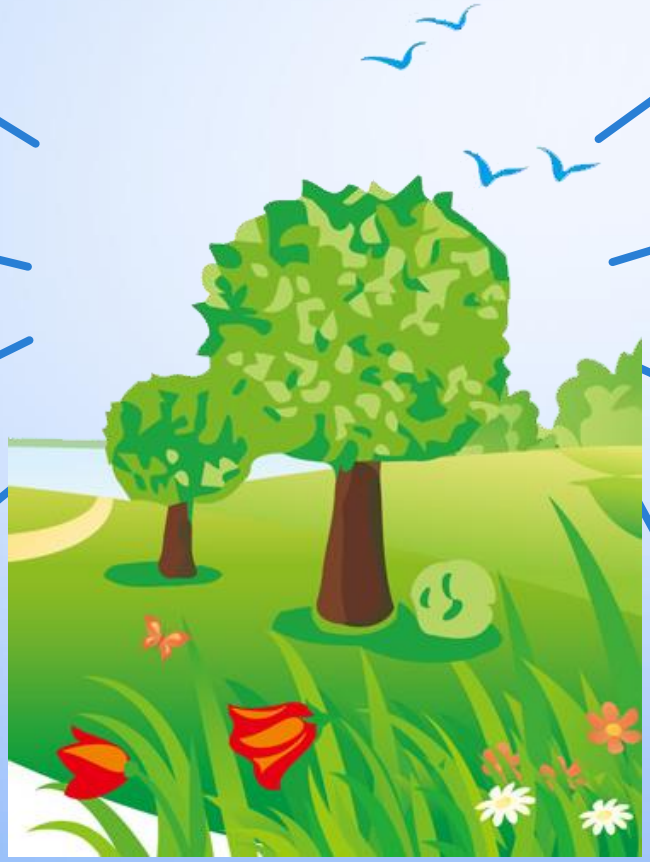
IOT-生活

無人汽車

無人公車

無人送餐機

ETC



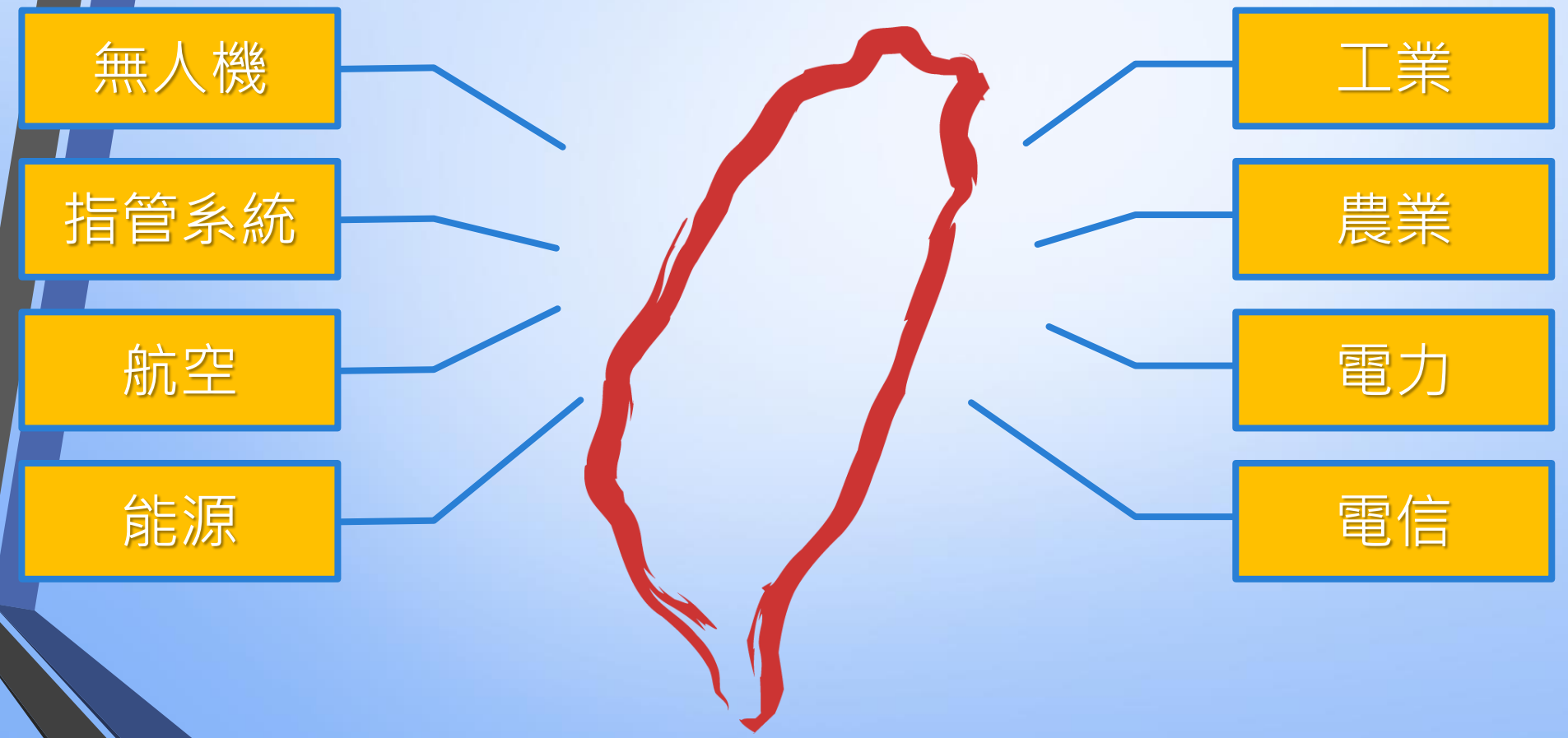
智慧電網

智慧馬路

路口監視

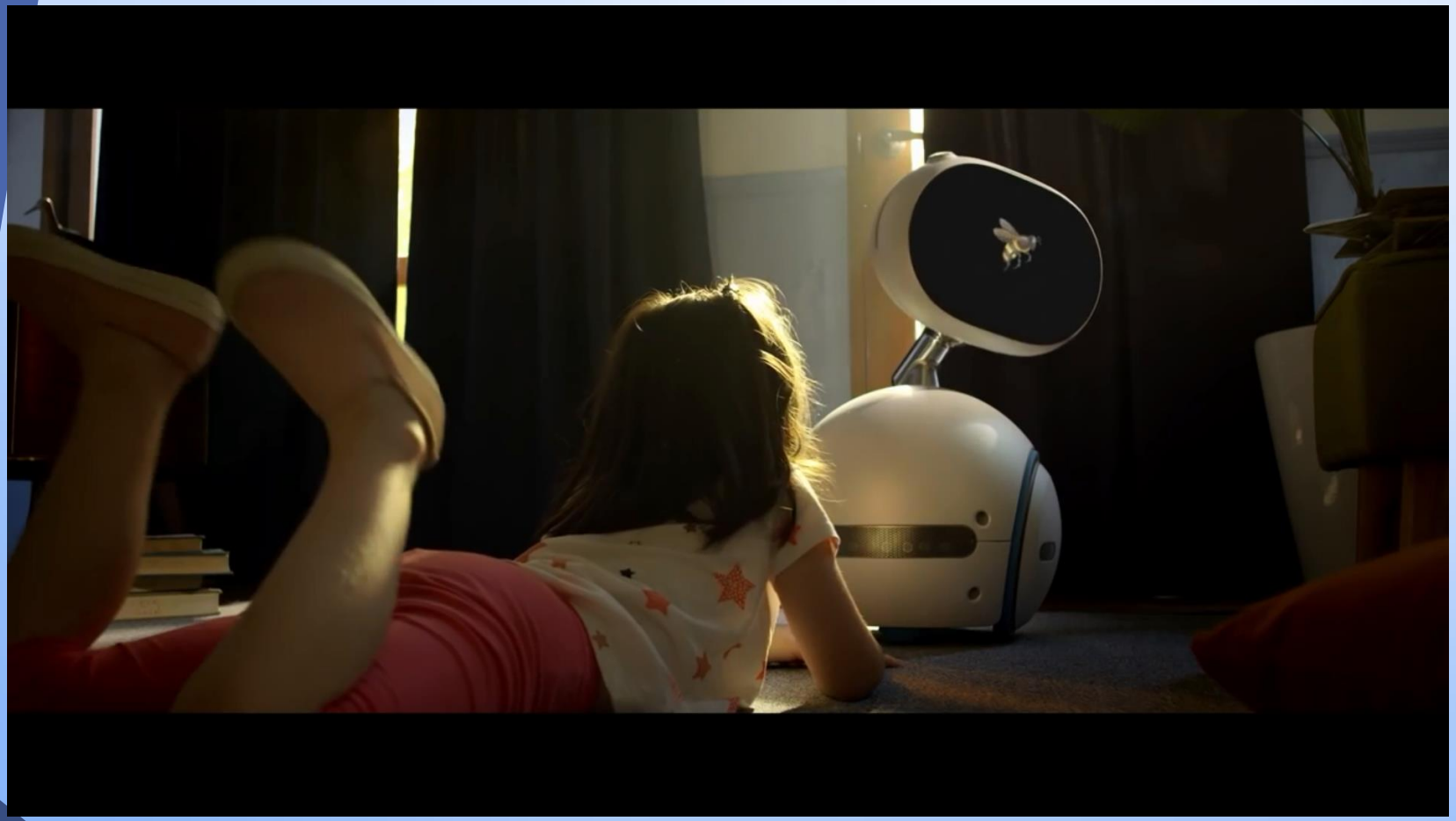
智慧交通
(高鐵、台鐵、捷運、公車、流量)

IOT-社會



智能管家

資料來源：https://www.youtube.com/watch?v=KHZPVVlGmBQ



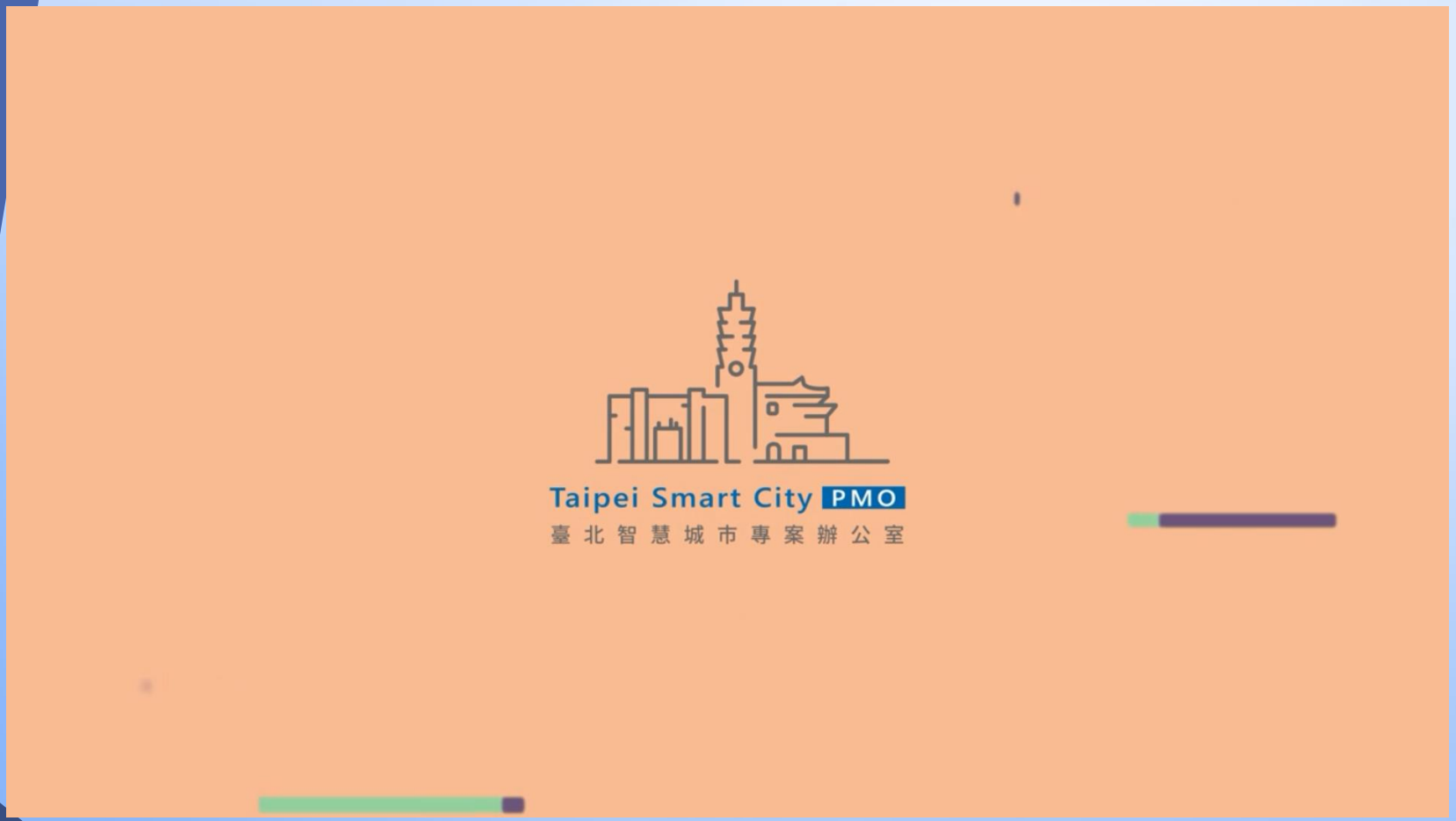
資料來源：https://www.youtube.com/watch?v=CxyGA_siMWg

智能家庭

資料來源：https://www.youtube.com/watch?v=lOjCN8cSCZ8

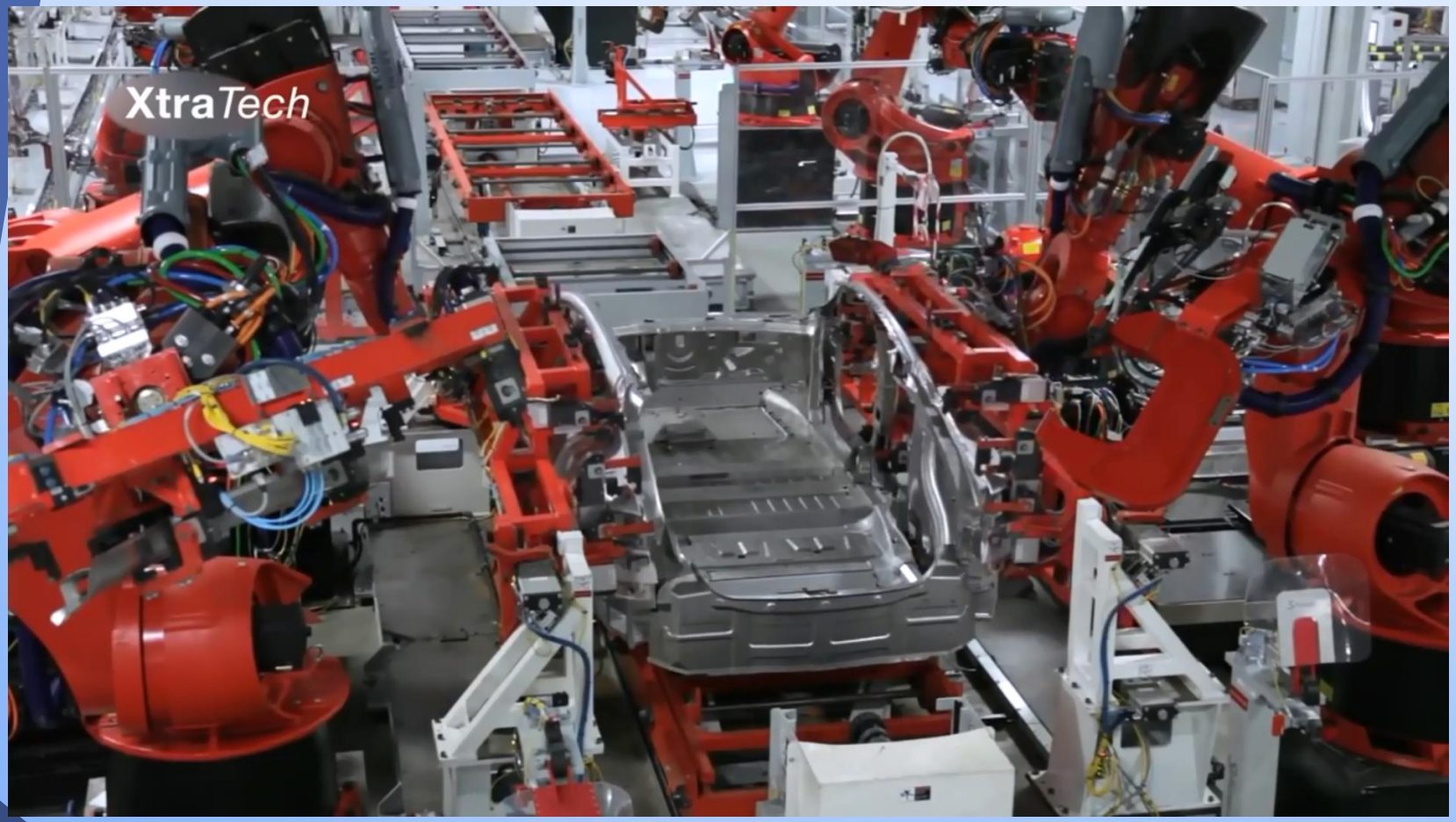
資料來源：https://www.youtube.com/watch?v=UnBNS_Yoc8g

智慧城市



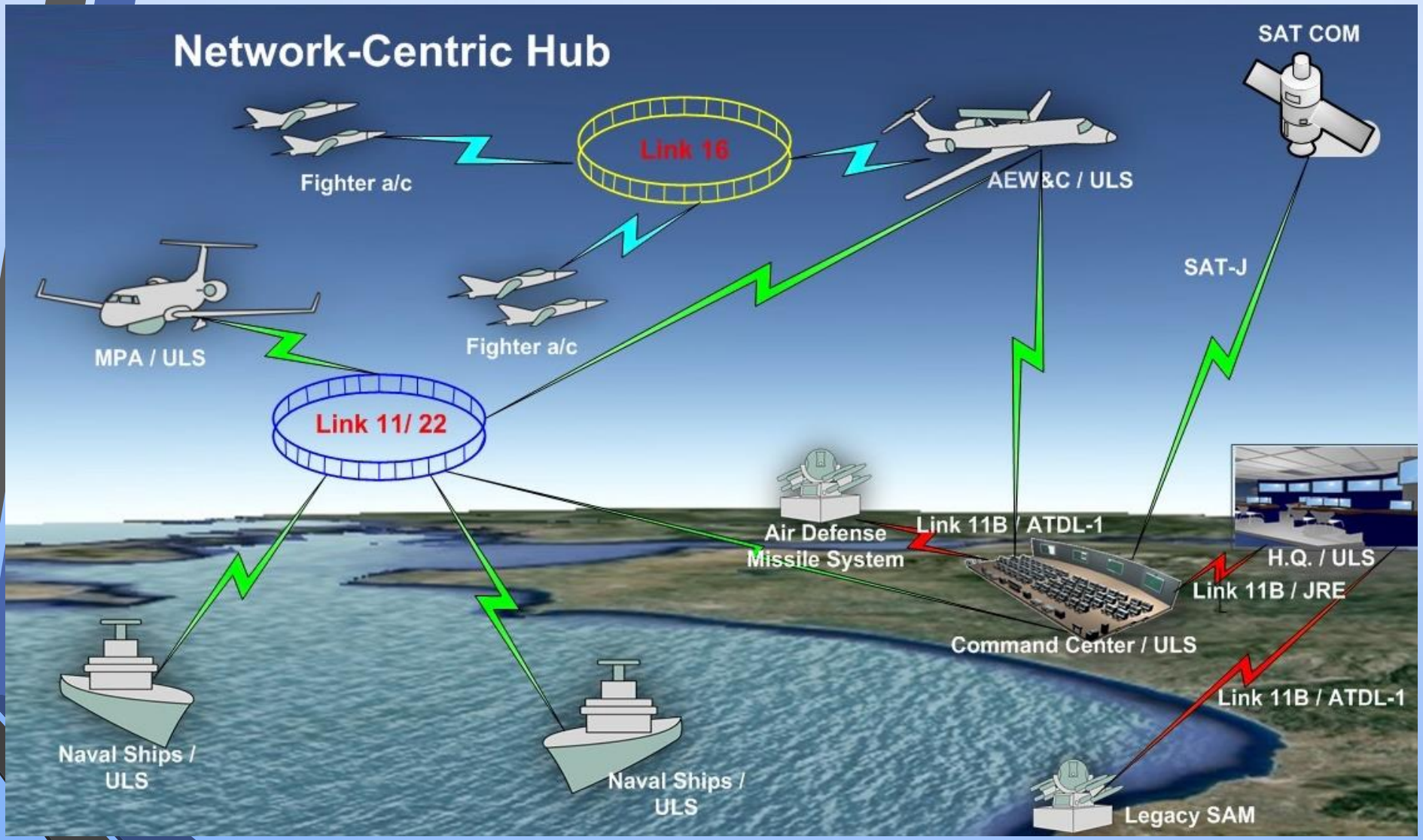
資料來源：https://www.youtube.com/watch?v=u0eaRrrS_RI

智能工廠



資料來源：https://www.youtube.com/watch?v=RuYKkNlCQag

國防指管系統



資料來源：http://www.dwarsliggers.eu/index.php/2016-04-01-13-52-07/algemeen/211-ncw-belgium

車聯網也有駭客危機? 萬物聯網成漏洞

資料來源：https://www.youtube.com/watch?v=s8cgrP-Hz0U

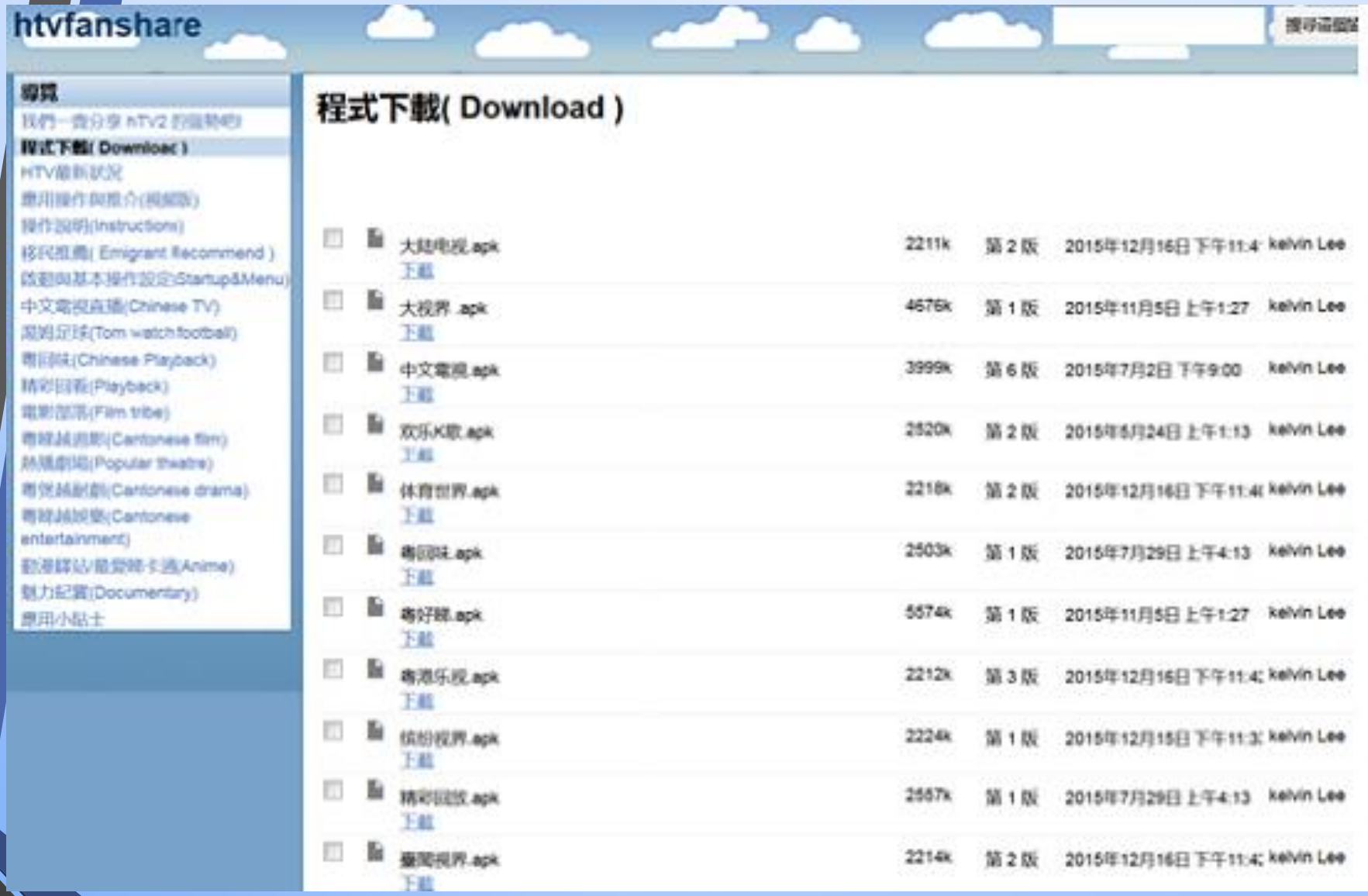
勒索病毒入侵智慧型聯網電視

- 使用智慧聯網電視大量進行音樂及遊戲下載的使用者，將是受病毒感染的高危險群。
- 受到感染後的症狀，就是電視螢幕突然停止了正常的轉動，然後螢幕上會出現以日文或英文表示「要恢復正常，請繳交一萬日圓！」的訊息。
- 必須透過購買蘋果 iTunes 預付卡的方式支付款項，必且限定在 72 小時內支付，否則該智慧聯網電視將永遠被鎖定螢幕而無法正常運作。

資料來源：http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/
http://technews.tw/2016/10/31/smart-tv/

◆ 散布智慧型電視惡意程式的網站畫面。

資料來源：http://blog.trendmicro.com.tw/?p=9254



◆ 散布智慧型電視惡意程式的網站畫面。

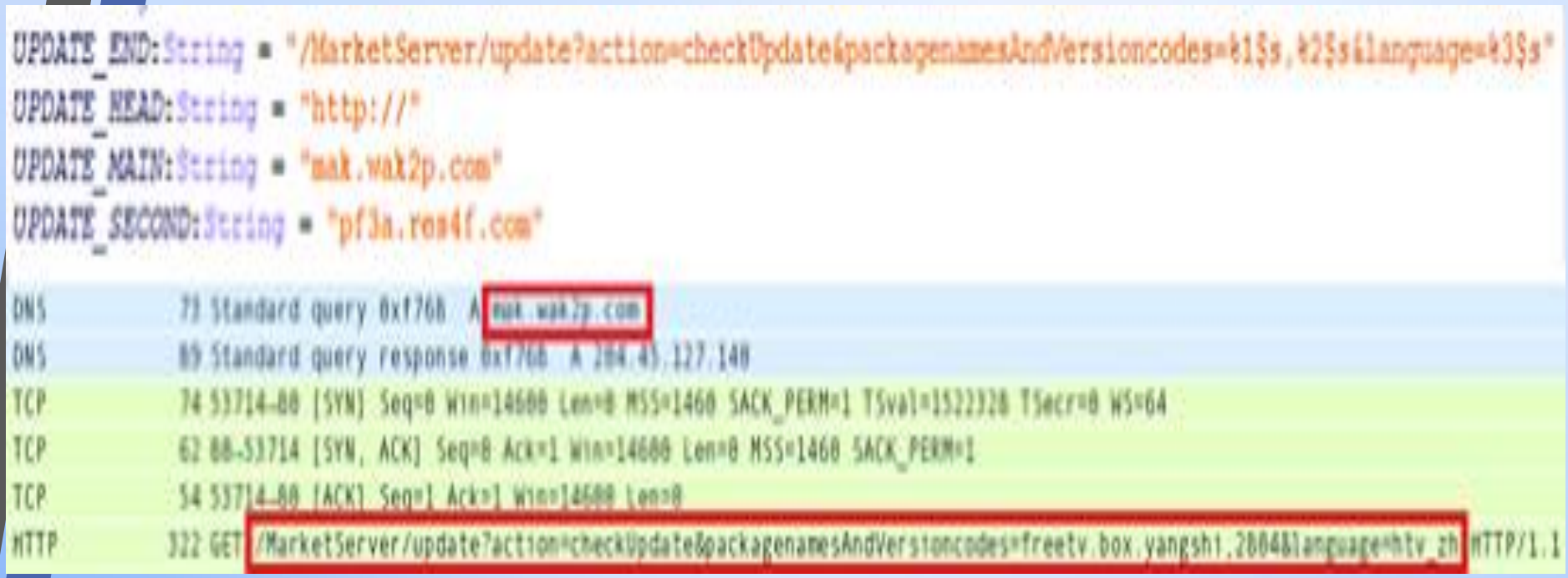
資料來源：http://blog.trendmicro.com.tw/?p=9254

```
public class InstallApk {
    public InstallApk() {
        super();
    }

    public static void execCommand(String arg2) {
        new Thread(new Runnable() {
            public void run() {
                Process v2;
                String v0 = "pm install -r " + this.val$path;
                Log.i("UpdateHelper", "安裝apkpath==" + this.val$path);
                try {
                    v2 = Runtime.getRuntime().exec(v0);
                    Log.i("UpdateHelper", "安裝apk");
                    v2.waitFor();
                }
                catch(Throwable v3) {
                    try {
                    label_33:
                        v2.destroy();
                    }
                    catch(Exception v1) {
```

- 應用程式偷偷安裝其他惡意程式。

資料來源：http://blog.trendmicro.com.tw/?p=9254



- 惡意程式從遠端更新應用程式。

資料來源：http://blog.trendmicro.com.tw/?p=9254

資料來源：http://blog.trendmicro.com.tw/?p=9254

資料來源：http://blog.trendmicro.com.tw/?p=9254

IOT之資安防範

- 啟用智慧型設備上所有的安全功能。
- 購買會定期更新產品韌體的廠商出的物聯網產品。
- 研究自己的智慧型設備是否能夠正確地加密其韌體更新和網路通訊。
- 使用安全的密碼。
- 了解製造商如何管理他們的設備漏洞。

資料來源：https://blog.trendmicro.com.tw/?p=11690

簡報大綱

- 個資暨資安案例分享
- 2017年資安預測
- 釣魚郵件與網站介紹與防護
- 物聯網(IoT)資安
- 勒索軟體介紹與防護

美連鎖醫院MedStar疑遭勒索軟體攻擊，病人被迫轉院

- MedStar未公開說明是否遭到勒索軟體攻擊，但員工爆料在電腦上看到駭客勒索的視窗畫面，要求醫院支付45個比特幣，相當於1.9萬美元，以換取資料解密。MedStar遭攻擊後，關閉所有電腦系統與電子郵件，迫使部分病況緊急的病人必須轉院治療，不須轉院的病人則以傳統的紙筆作業進行病歷登錄。
- 最後院方與駭客妥協支付1.7萬美元，才使系統恢復正常。

資料來源：http://www.ithome.com.tw/news/105077

臉書釣魚影片又來了，假冒好友私訊騙你植入勒索軟體Locky

- 駭客先假冒朋友的Facebook帳號，透過私訊傳送內藏特殊腳本程式的偽造svg圖片檔給勒索對象，這個偽造圖片會打開一個假冒的Youtube網頁，並跳出安裝下載開啟一個內藏有Nemucod惡意程式的Chrome外掛程式「One」的請求。

資料來源：http://www.ithome.com.tw/news/109738

舊金山交通局遭勒索軟體攻擊

- 美國舊金山市交通局遭到駭客以勒索軟體攻擊，並造成售票系統一度停擺， 外傳駭客向SFMTA勒索了100個比特幣（約7.3萬美元），SFMTA本周公開對外說明了此事，雖未證實勒索金額。
- 仰賴內部的IT團隊利用備份功能回復系統。

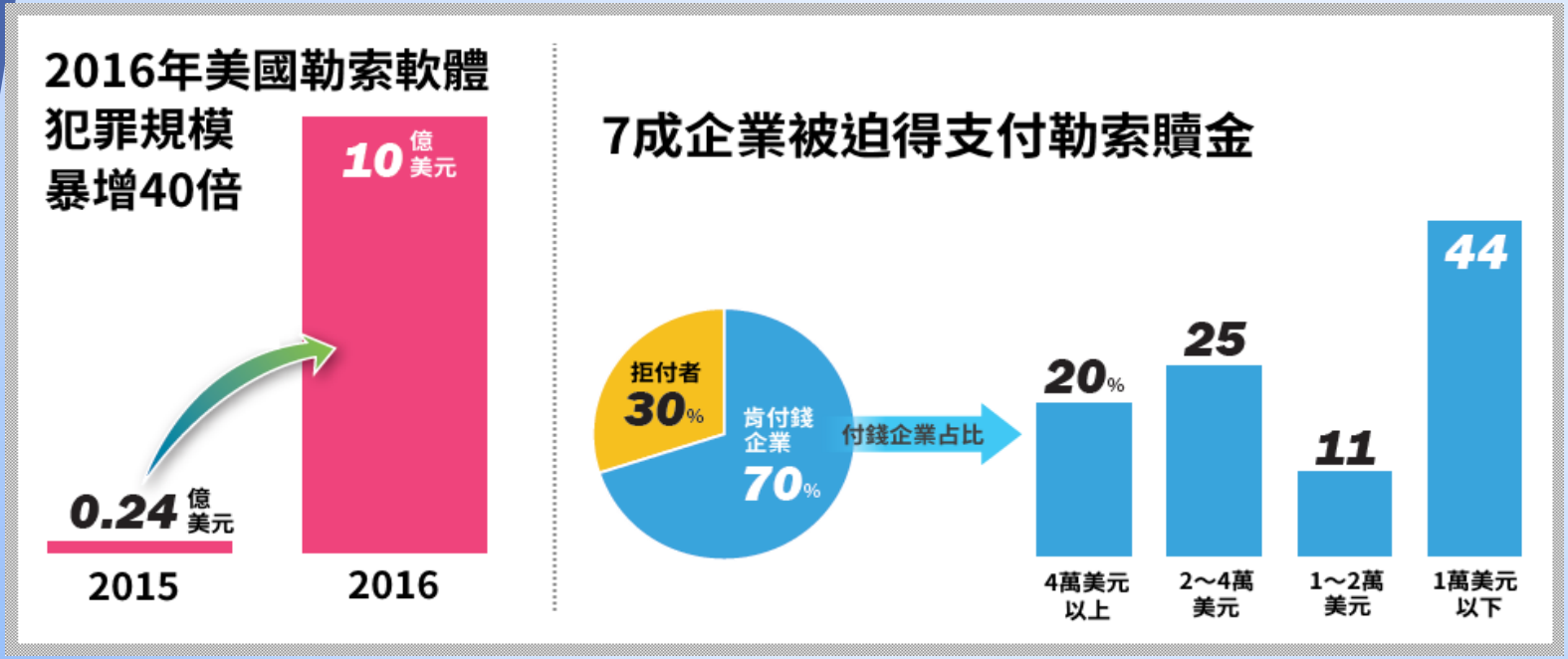
資料來源：http://www.ithome.com.tw/news/109939

奧地利一飯店因勒索軟體癱瘓電子門鎖系統，準備回到傳統鑰匙門鎖

- 由於飯店的電腦遭到勒索軟體加密，使得該飯店的訂房、收銀、電子門鎖等系統無法使用，最後飯店決定支付2個比特幣，以換取駭客解密電腦。
- 該飯店已決定在下次將電子門鎖換裝回傳統鑰匙門鎖。

資料來源：http://www.ithome.com.tw/news/111588

2017資安趨勢 勒索軟體風暴狂襲



- 美國FBI評估，2016年勒索軟體美國網路犯罪規模超過10億美元，相較2015年全年勒索軟體犯罪規模只有2,400萬美元，成長超過40倍。
- 勒索軟體危害在2016年達到高峰，除了出現勒索軟體即服務（Rabsomware-as-a-service）或是拉2位下線可免費解密的營運模式外，勒索軟體綁架對象已經從傳統電腦和伺服器，擴散到手機及智慧連網電視等新興連網裝置。

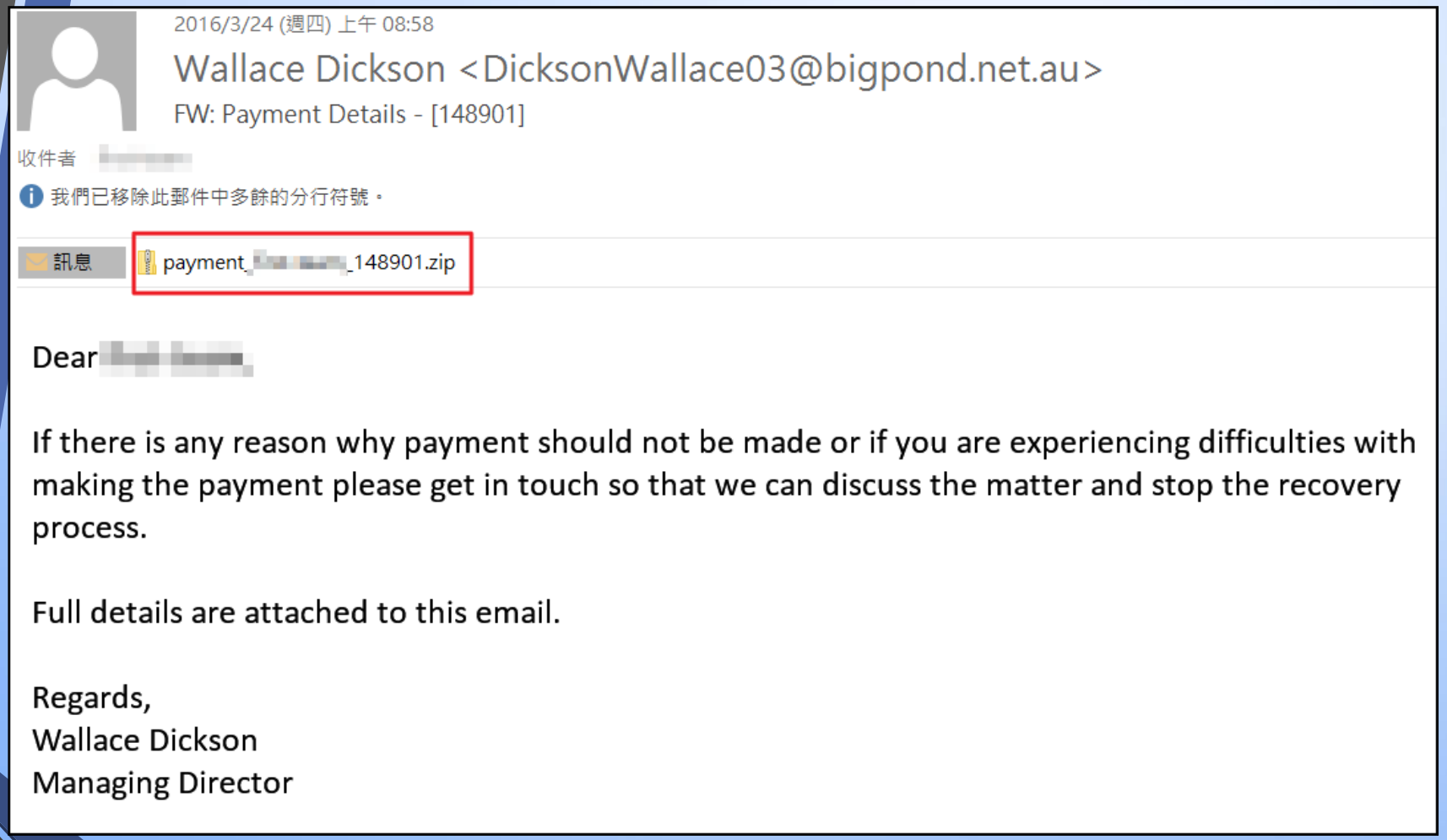
資料來源：http://www.ithome.com.tw/news/111219

勒索病毒DIY 套件,削價競爭, 只要 39 美元,終生授權!

- 最近，RaaS 的價格又再度開始滑落，原因是，當勒索病毒的需求不斷成長之後，已有更多的病毒作者紛紛投入這塊市場，進而導致競爭激烈，價格隨之下滑。

資料來源：https://blog.trendmicro.com.tw/?p=25625

新型態的加密勒索惡意程式分析



2016/3/24 (週四) 上午 08:58

Wallace Dickson <DicksonWallace03@bigpond.net.au>

FW: Payment Details - [148901]

收件者 [redacted]

我們已移除此郵件中多餘的分行符號。

訊息 payment_[redacted]_148901.zip

Dear [redacted]

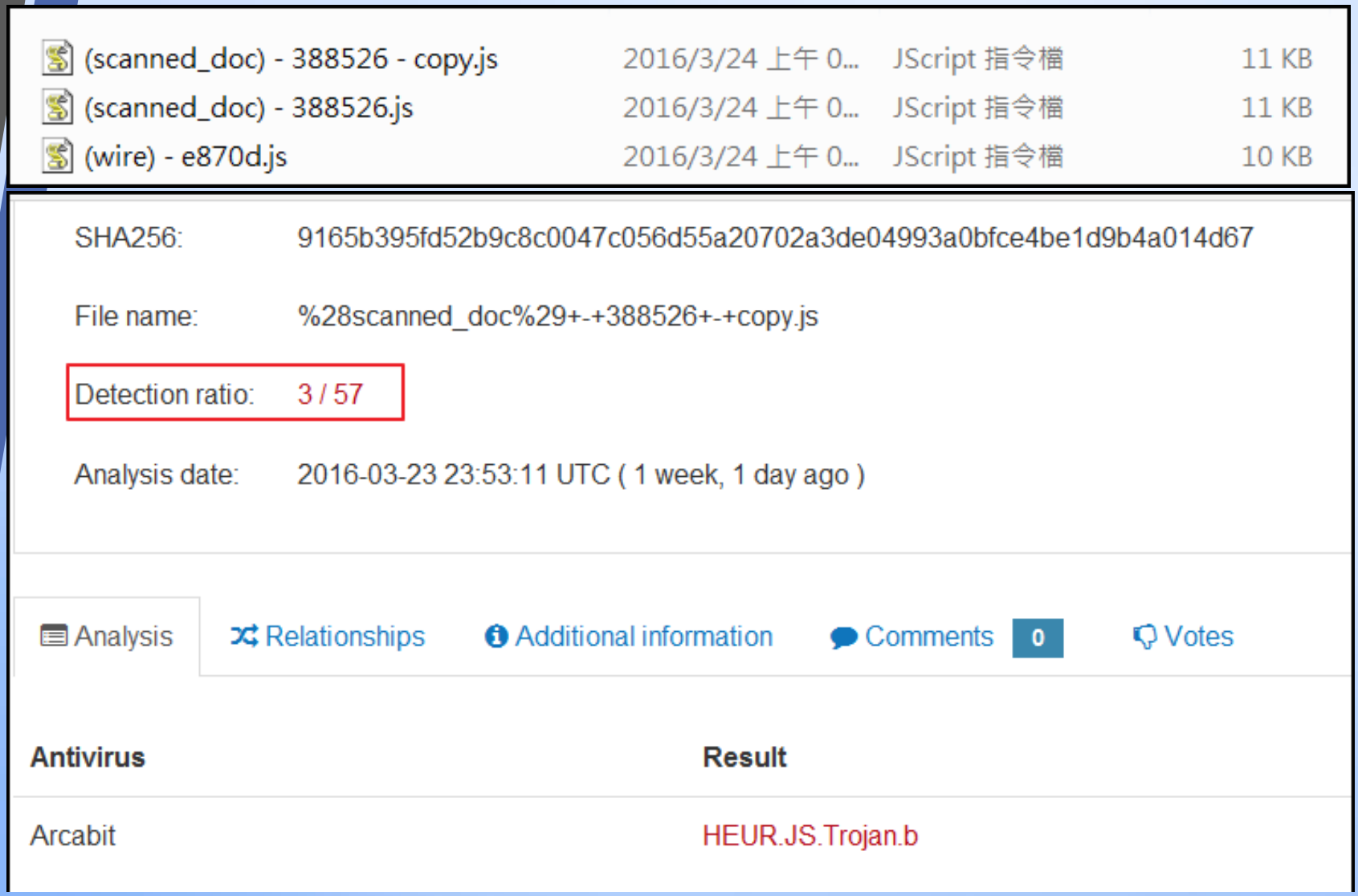
If there is any reason why payment should not be made or if you are experiencing difficulties with making the payment please get in touch so that we can discuss the matter and stop the recovery process.

Full details are attached to this email.

Regards,
Wallace Dickson
Managing Director

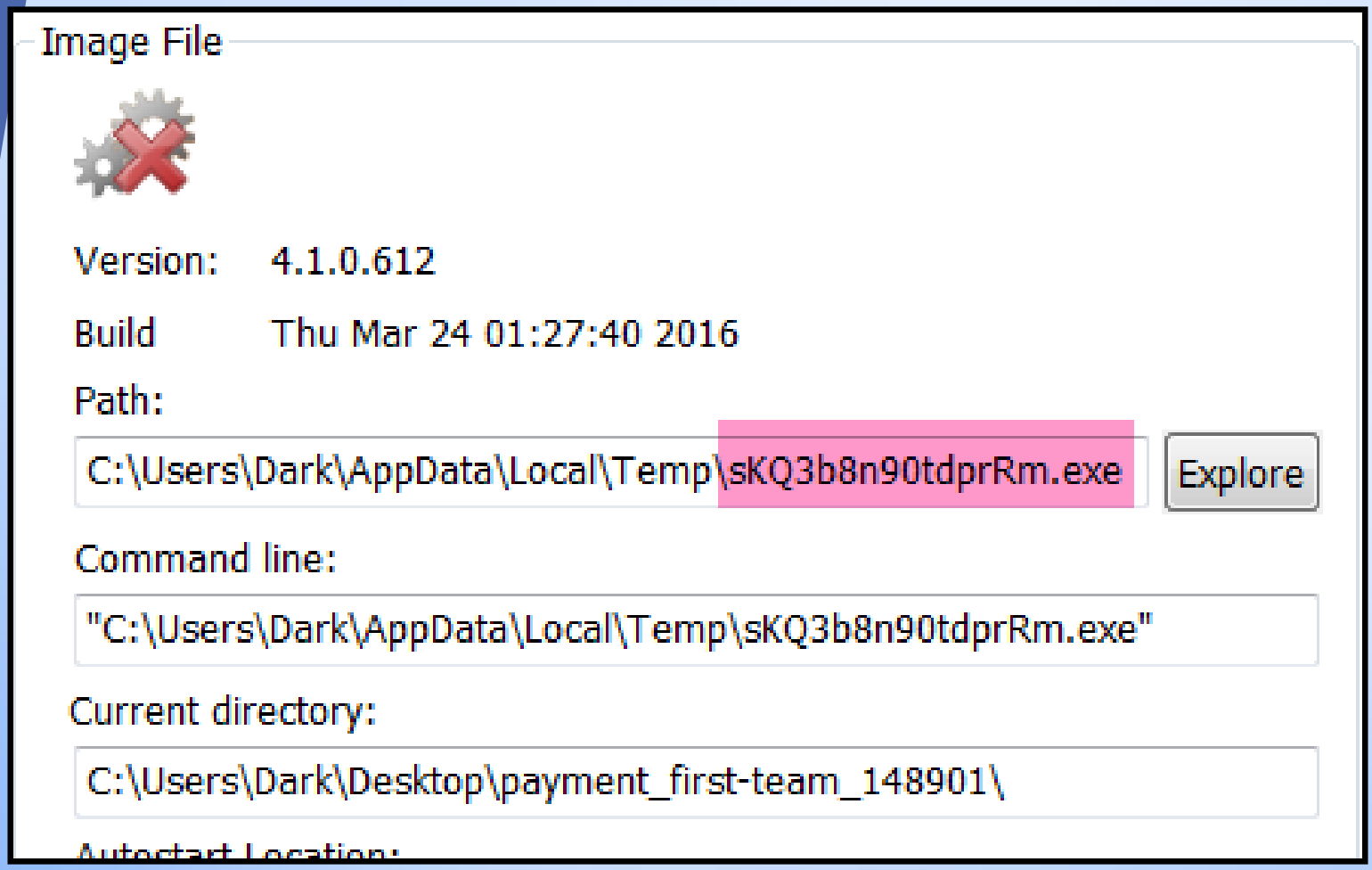
- 此例中的郵件主旨是要求檢查收款資訊 ，並夾帶 zip 的壓縮檔案。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心



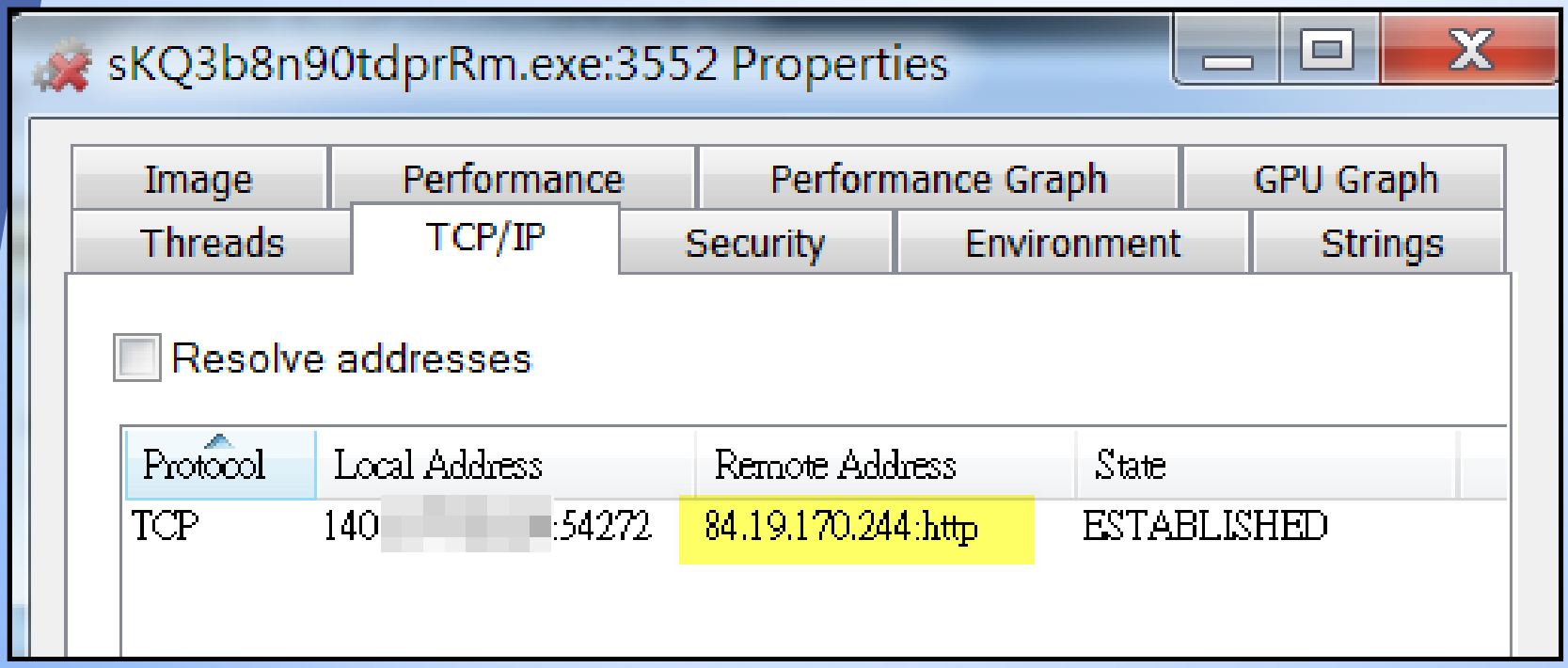
- 惡意程式 zip 解壓縮之後會有三個附檔名為 js 的檔案，雖然並非常見的 exe 檔案， js 事實上是用 javascript 撰寫的執行檔案。
- 三個 JS 執行檔病毒的檢測比例 3/57，為新型態的加密勒索軟體。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心



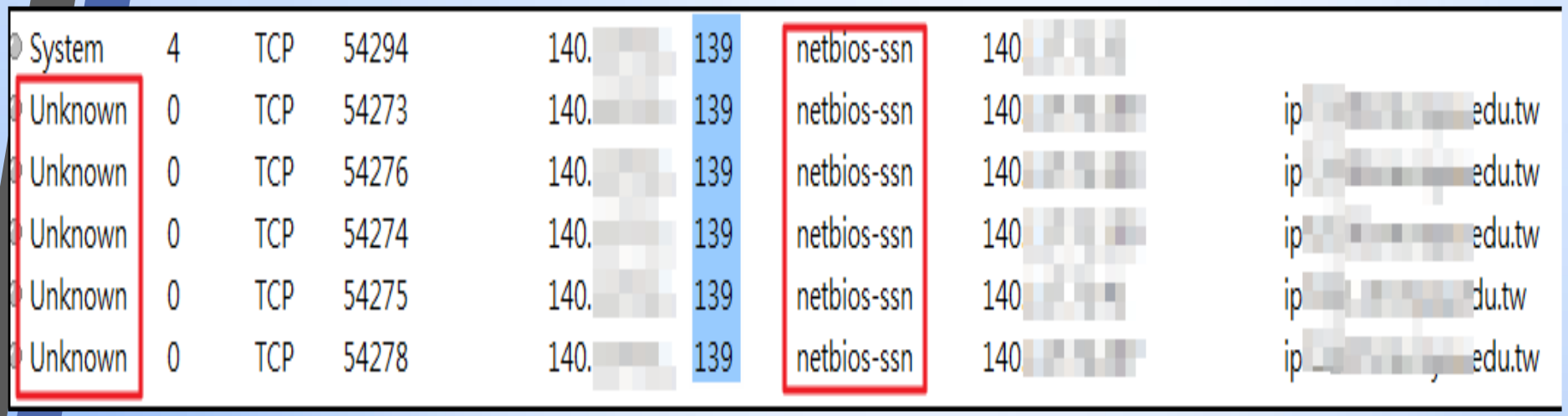
- 首先執行 js 的檔案，系統會使用預設 java script 程式去執行。
- 位於隱藏路徑中 \AppData \Local \Temp \ 的 sKQ3b8n90tdprRm.exe 惡意程式正在執行，而該程式就是透過原本的 js 檔案產生的。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心



- 查看該惡意程式 sKQ3b8n90tdprRm .exe 的網路狀態可以發現，正在對外部 84.19.170.244 的網路連線，該 IP 位址於 RU 俄羅斯國家。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心



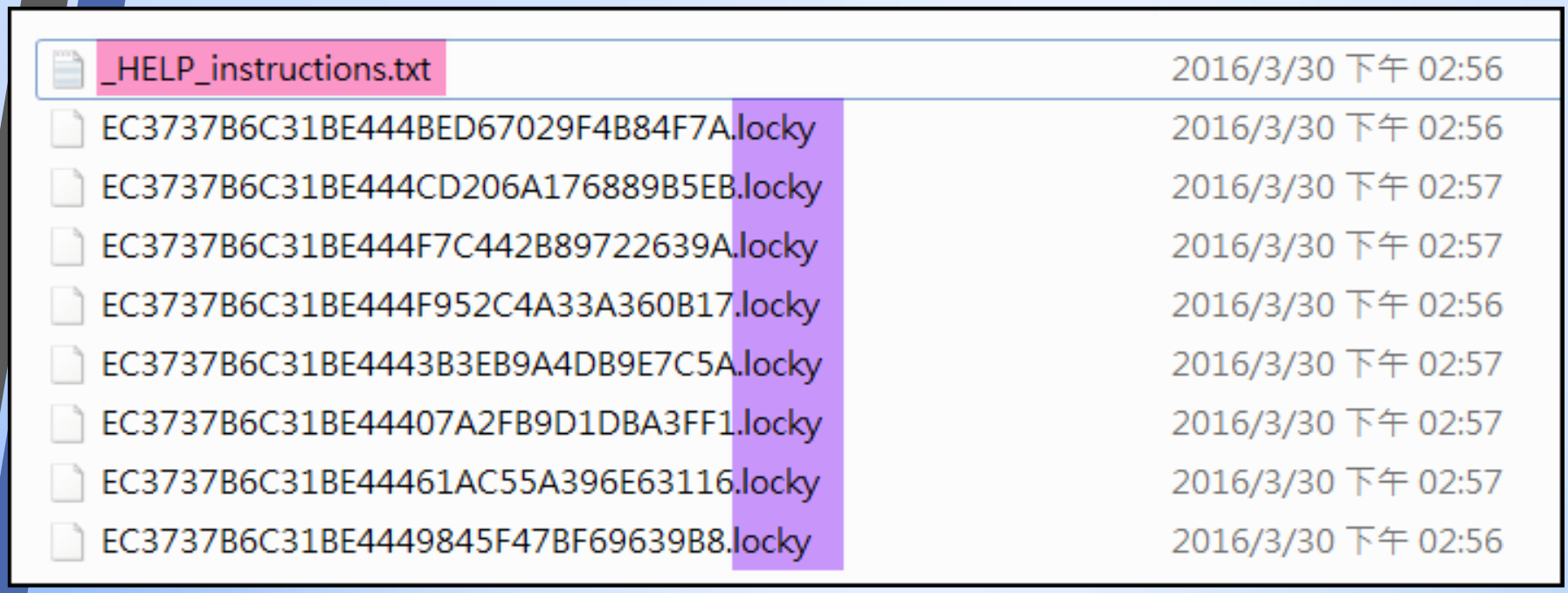
System	4	TCP	54294	140.	139	netbios-ssn	140	
Unknown	0	TCP	54273	140.	139	netbios-ssn	140	ip edu.tw
Unknown	0	TCP	54276	140.	139	netbios-ssn	140	ip edu.tw
Unknown	0	TCP	54274	140.	139	netbios-ssn	140	ip edu.tw
Unknown	0	TCP	54275	140.	139	netbios-ssn	140	ip du.tw
Unknown	0	TCP	54278	140.	139	netbios-ssn	140	ip edu.tw

- 該程式除了對外 IP 建立連線，也會針對內部網段其他 IP 進行 scan 動作，判斷為找尋可存取的網路檔案進行檔案加密。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心

- 當所有磁碟內部或外部的關聯檔案都被加密後，桌面會跳出一個圖片檔「_HELP_instructions.bmp 」以及一個「 _HELP_instructions.txt 」說明 」說明檔，主要內容是引導被害者如何進行繳付勒索贖金，此時所有可開啟文件都已經無法開啟 。。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心

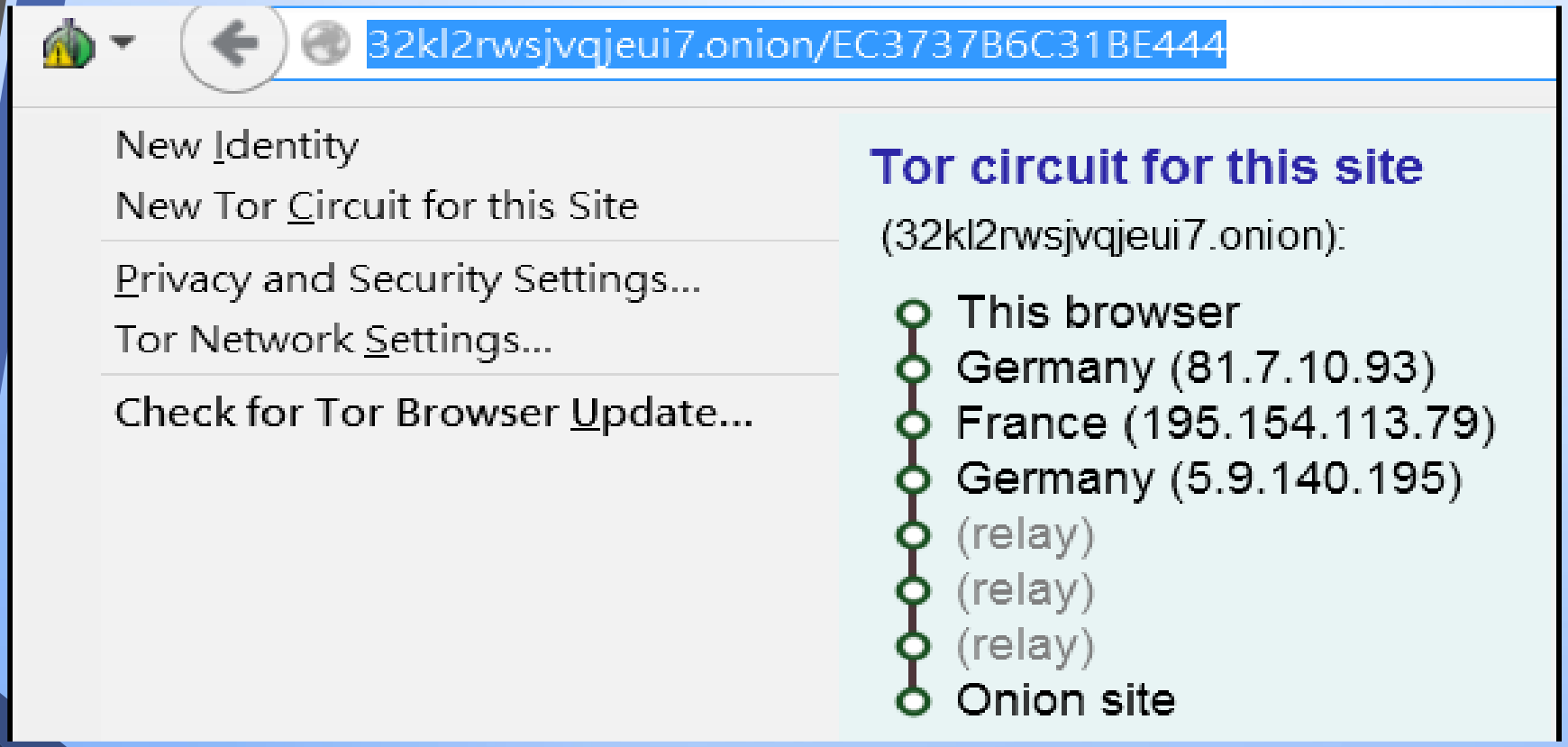


- 此時隨意開啟資料夾查看原有文件檔，發現所文件檔的確都被置換檔案名稱以及副檔為 locky ，並附上一個贖金引導的 txt 說明檔，其內容同於黑底紅字的圖片內容。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心

只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。
如要接收您的私人金鑰，請點擊以下其中一個連結：

1. http://32kl2rwsjvqjeui7.tor2web.org/EC3737B6C31BE444
2. http://32kl2rwsjvqjeui7.onion.to/EC3737B6C31BE444
3. http://32kl2rwsjvqjeui7.onion.cab/EC3737B6C31BE444



- 此例開啟特殊 onion 網域位址後看到至少經過三次的 Relay IP ，才轉跳至未知的目地 onion site 。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心

使重新页并下载解码软件。

接收确认比特币交易后，您会被重定向到下载解码软件的页。

- 透過 Tor 瀏覽器成功開啟網址後，出現簡體中文Locky Decryptor 網頁，意思是受害者必須向該站購買解密的金鑰程式，才能還原被加密過的檔案，並且必須透以比特幣作為支付方式將 0.5 BTC 付款至指定位址，大約是 7000 台幣 。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心

SHA256: 7a6cf27dda962107e9b439c25c95db92e13f3587985eea656185a49ed1f4a72f

File name: 2.exe

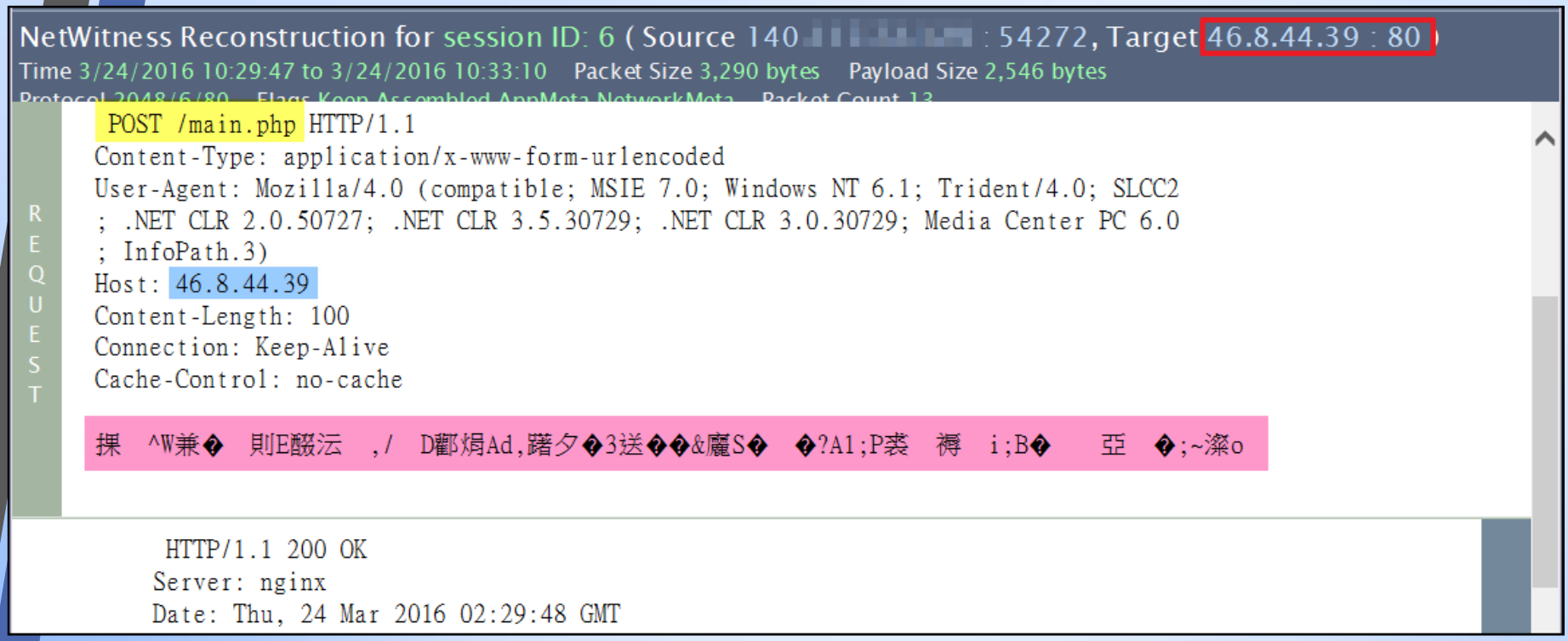
Detection ratio: 46 / 57

Analysis date: 2016-04-05 14:53:55 UTC (10 hours, 57 minutes ago)

Antivirus	Result
ALYac	Trojan.Ransom.LockyCrypt
AVG	Crypt5.ASCM
AVware	Trojan.Win32.Generic!BT
Ad-Aware	Trojan.GenericKD.3118559

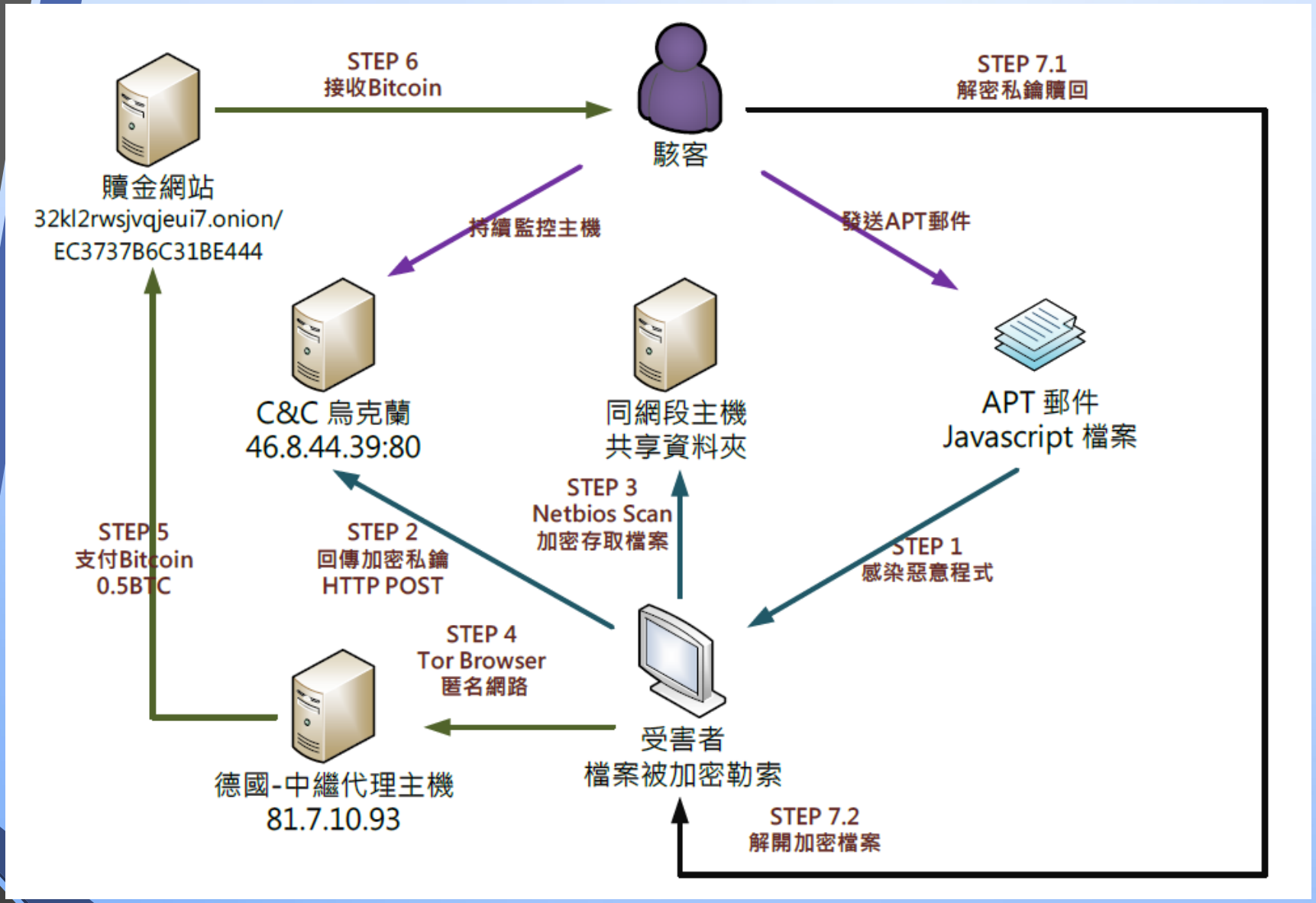
- 所有檔案被加密後，原本的惡意程式 js 檔案和 sKQ3b8n90tdprRm .exe 檔案也都會自我移除。
- 透過 Virustotal掃描 sKQ3b8n90tdprRm .exe 可以很清楚看到是高偵測比例 46/57 的勒索軟體，檢測名稱是 2. exe 。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心



- 從網路封包中可以看到，主機感染惡意程式一開始會連到烏克蘭的 C&C 主機「46.8.44.39」，並且透過 HTTP POST 方式將加密內容送出，判定可能是勒索加密的私鑰。
- 當主機向上層 C&C 報到並送出私鑰後，惡意程式開始對內部網路進行 netbios 的掃瞄，並嘗試針對能夠存取共享資料夾進行加密，若有連接網路磁碟或 NAS 就有可能遭受破壞。

資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心



資料來源：新型態的加密勒索惡意程式分析報告，TACERT臺灣學術網路危機處理中心

您如何避免自己成為勒索軟體的受害者？

- 開啟電子郵件之前請先仔細看清楚
- 避免點選不明來源電子郵件內的連結
- **備份、備份、備份**您的重要檔案

課後評量

BCCS 漢昕科技

謝謝聆聽

Thank you