

近期駭客攻擊案例分享

行政院國家資通安全會報 技術服務中心

- 趨勢探討

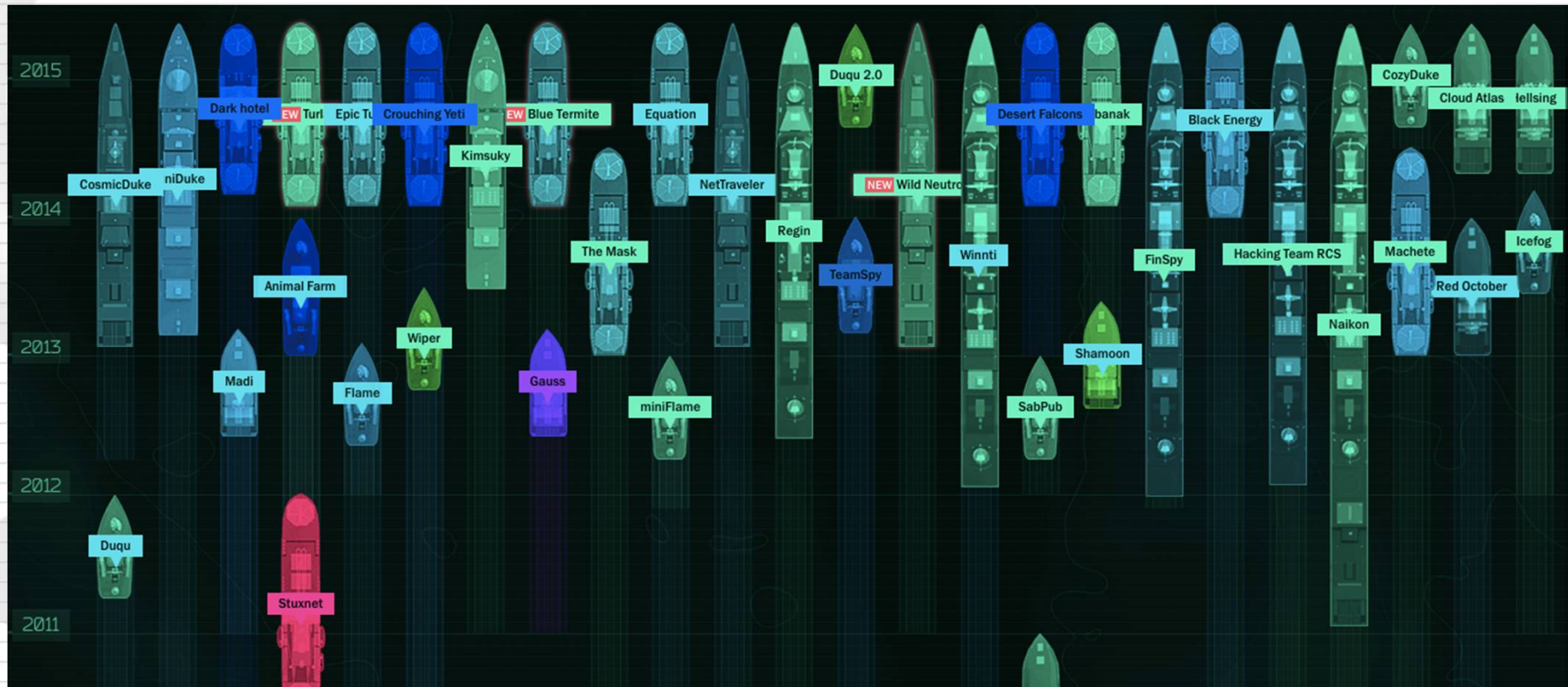
- APT依然是政府機關主要的資安威脅
- 複合式攻擊：Zero-day軟體漏洞+社交工程郵件

- APT攻擊案例分享

- 零時差弱點攻擊案例
- 網路設備被當中繼站案例
- Golden ticket案例
- 第三方程式案例

- 結論與建議

- 2014 ~ 2015年間有超過20個APT駭客團體在全球活躍
- 除了美國、英國、中國、蘇聯、以色列等國，許多新興的APT團體來自北韓、中東等國家

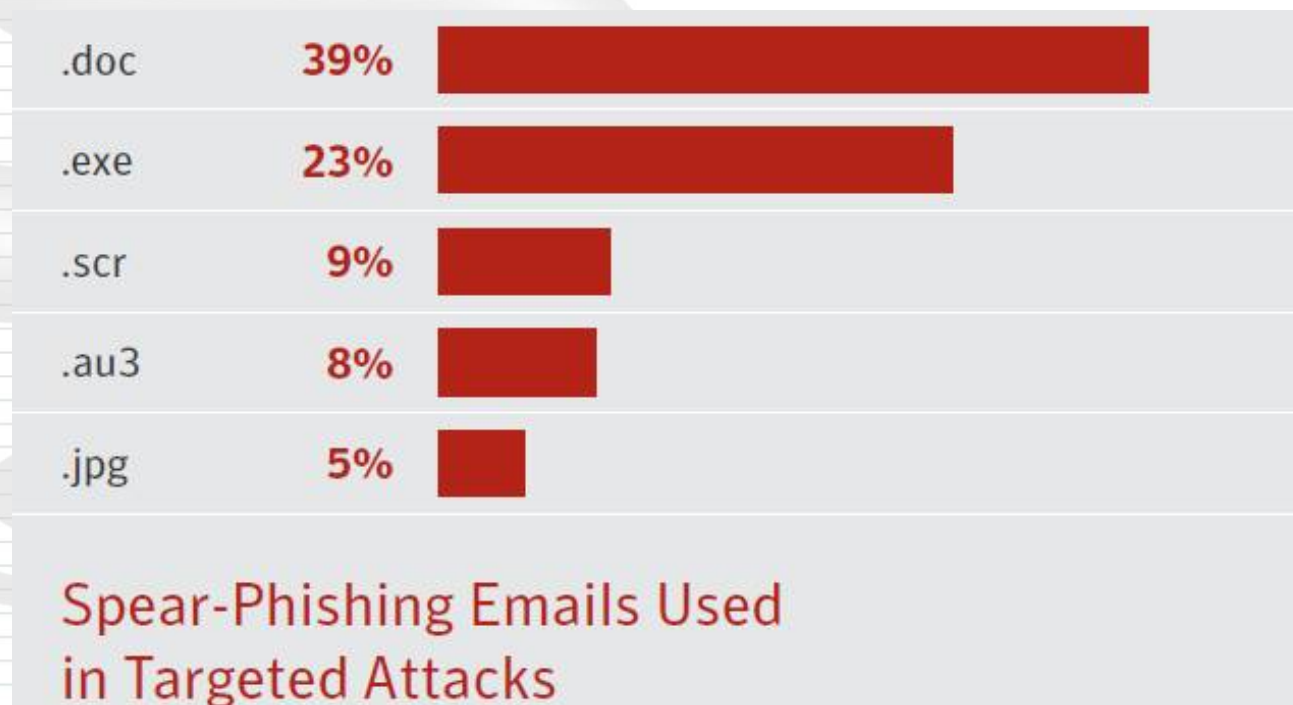


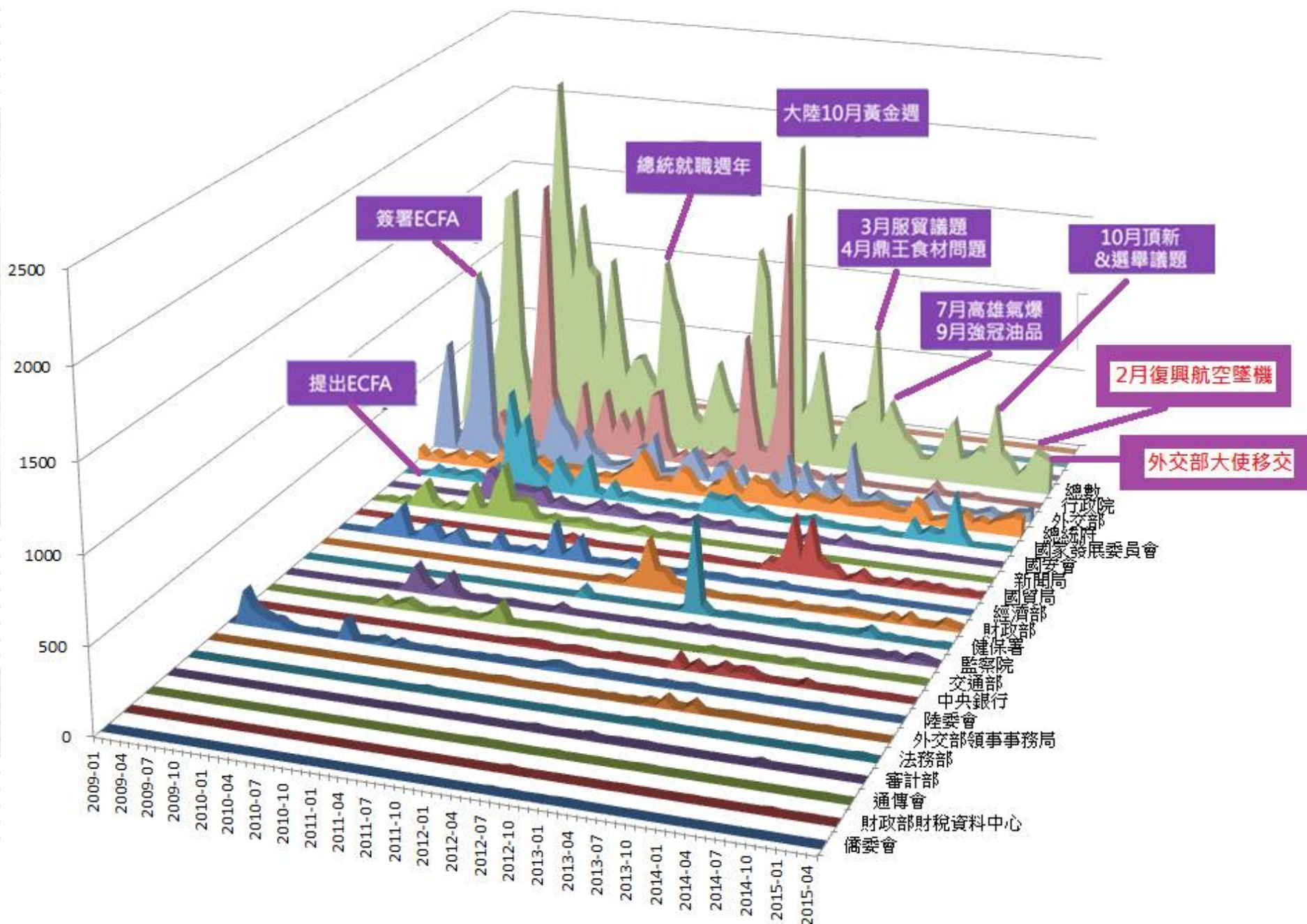
資料來源：<https://apt.securelist.com/>

● APT攻擊分析

–91%從Spear Phishing Email展開

- Spear Phishing Email中有94%帶有附件
- 附件類型包含.doc 、 .exe 、 .scr 、 .au3 、 .jpg 、 .pdf等





● APT攻擊依舊難以察覺

— 平均要花205天才會發現

How Compromises Are Being Detected



Time from Earliest Evidence of Compromise to Discovery of Compromise



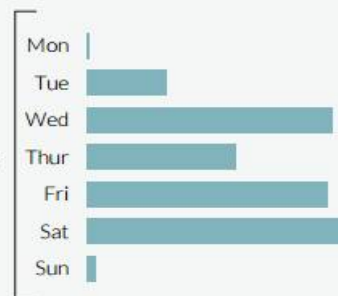
↓ 24 days less than 2013

Longest Presence: 2,982 days

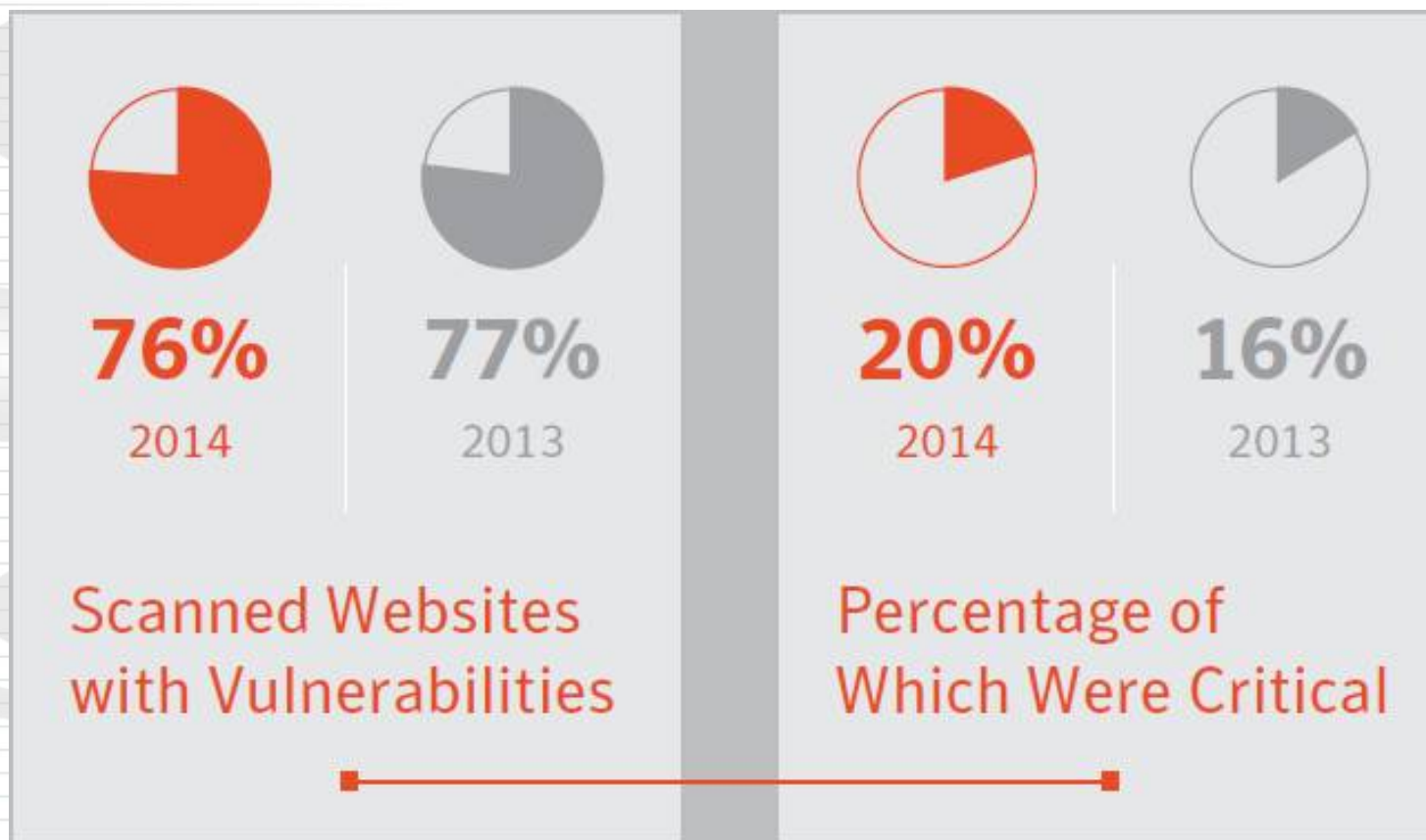
APT Phishing



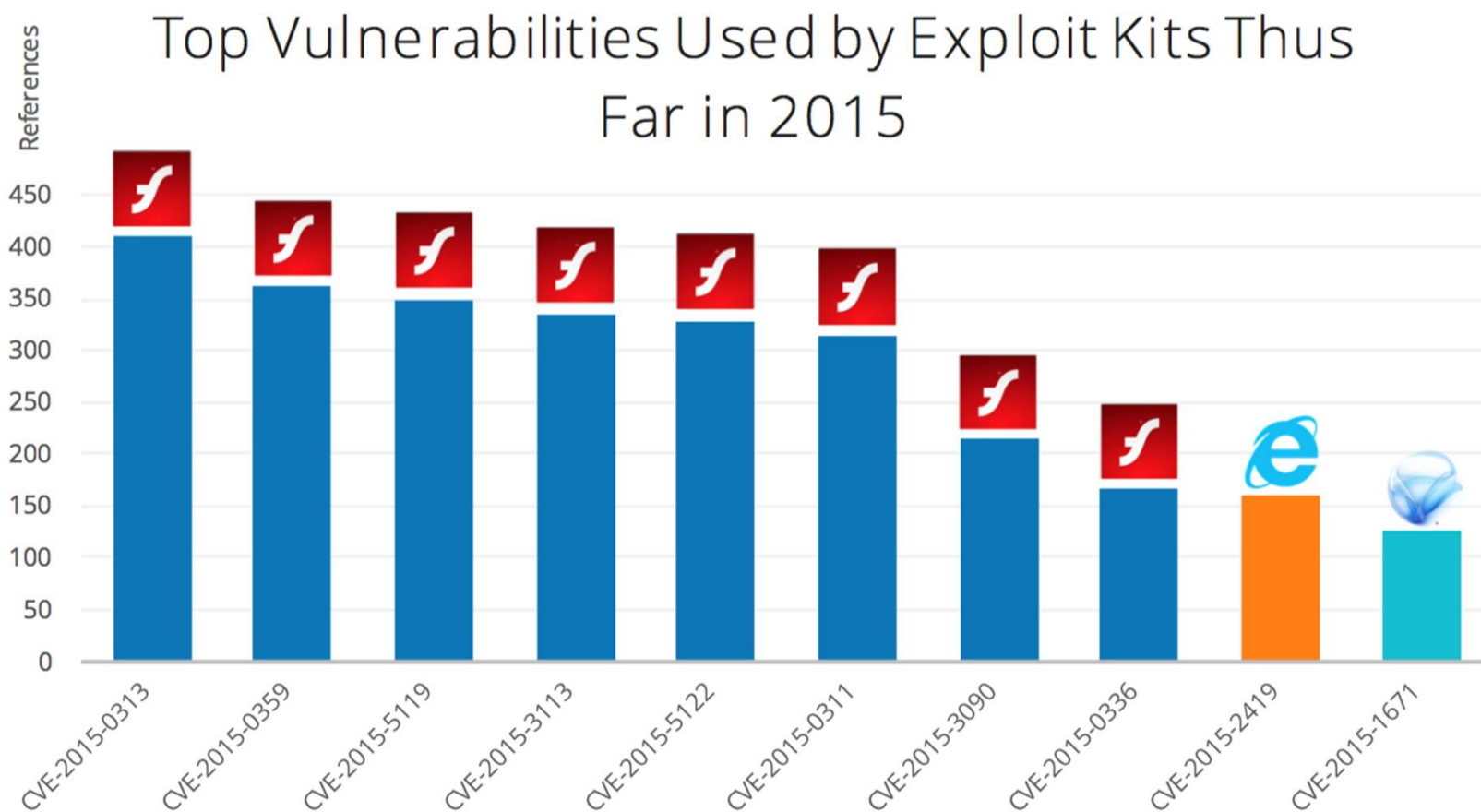
72%
of phishing emails were sent on weekdays



- 目前全世界大多數的網頁依然存在漏洞
 - 由於網頁的套件更新不易，加上部分網頁維護者資安意識不足，因此至今還是有多數網頁存在漏洞



- 最常被使用的前10個漏洞
 - 這些漏洞較易觸發且效果較佳



- 趨勢探討

- APT依然是政府機關主要的資安威脅
- 複合式攻擊：Zero-day軟體漏洞+社交工程郵件

- APT攻擊案例分享

- 零時差弱點攻擊案例
- 網路設備被當中繼站案例
- Golden ticket案例
- 第三方程式案例

- 結論與建議

- 零時差弱點攻擊案例

– 這故事就要從HackingTeam這家義大利公司說起了



- 此公司主要銷售手機、電腦的遠端遙控程式
 - 根據2014年citizenlab的研究報告指出，客戶主要包含埃及、智利、沙烏地阿拉伯、哈薩克、墨西哥、蘇丹等國家的政府部門



- 銷售對象大都是政府部門
 - 很多國家的政府喜歡傾聽民意
 - 在資訊數位化的今天，想要監控Line、Skype等軟體並不容易
- 為什麼要買HackingTeam的產品
 - HackingTeam賣的遠端遙控程式方便、易用、好安裝
 - 要在別人的手機或電腦上安裝遠端控制軟體可是不簡單的
 - 這類軟體要做到易用必須下不少功夫

● HackingTeam去哪裡找這麼多zero-day 漏洞？

– 公司規模才40人左右，不太可能找出一堆漏洞

– 漏洞用買的話.....難道不會很貴嗎？

➤ 微軟今年在BlackHat舉辦找漏洞活動，獎品是XBOX one、Surface 3

我發現了一個漏洞

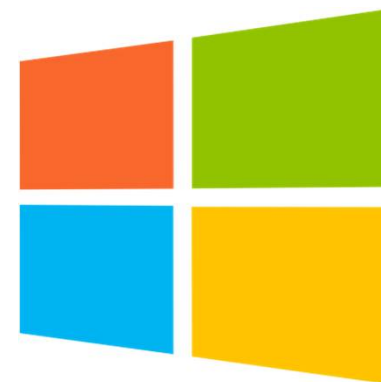


駭客

回報漏洞



賞你一台XBOX



微軟

- 駭客也是要養家活口的
 - 找漏洞並不是這麼容易的事情，但微軟只願用XBOX打發
 - HackingTeam知曉如何利用漏洞做生意，因此向駭客高額購買漏洞
 - 收購價格是50000~100000美金



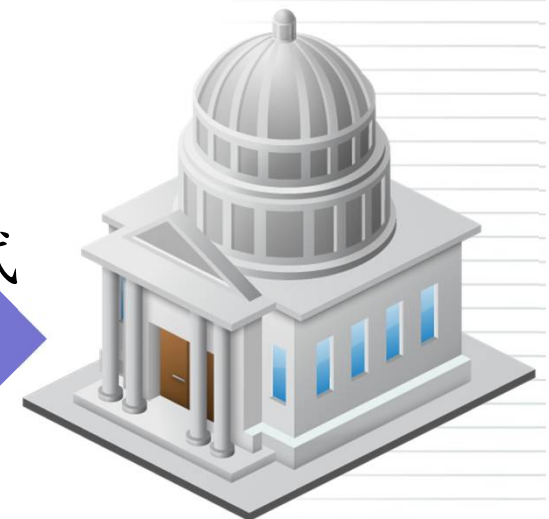
駭客

出售漏洞



HackingTeam

出售監控程式



政府

- 政府利用這些漏洞傾聽民意

- 透過漏洞與HackingTeam的強大管理架構，使得政府可以輕易地植入並監控受害者的行為

- 例如手機可監控GPS、相機、麥克風、簡訊、通話



- 中國已經示範給我們看了

A screenshot of a news article from iThome. The header is blue with the iThome logo on the left and a hamburger menu icon on the right. Below the header, there is a red tab labeled '新聞' (News). The main headline is in large, bold black characters. Below the headline, there is a paragraph of text in a smaller font. The background of the screenshot shows a faint, large 'ICST' watermark.

iThome

新聞

Lacoon：中國政府放出手機木馬間諜 程式監控香港佔中民眾

行動資安業者Lacoon表示，同時鎖定Android與iOS裝置的跨平台攻擊非常少見，應該可能有非常大型的組織或國家支撐。雖然先前市場也曾出現iOS木馬程式，但Xsser mRAT則是迄今最精密，功能也最強大的一款。

- 駭客中也有勇於維護自由的正義之士
 - 2015/7/5 HackingTeam遭駭客入侵，並公布所有資料

]HT[**Hacked Team**
@hackingteam

+ Follow

Since we have nothing to hide, we're publishing all our e-mails, files, and source code mega.co.nz/#!Xx1lhChT!rbB...
infotomb.com/eyyxo.torrent

RETWEETS
57

FAVORITES
32



5:26 PM - 5 Jul 2015

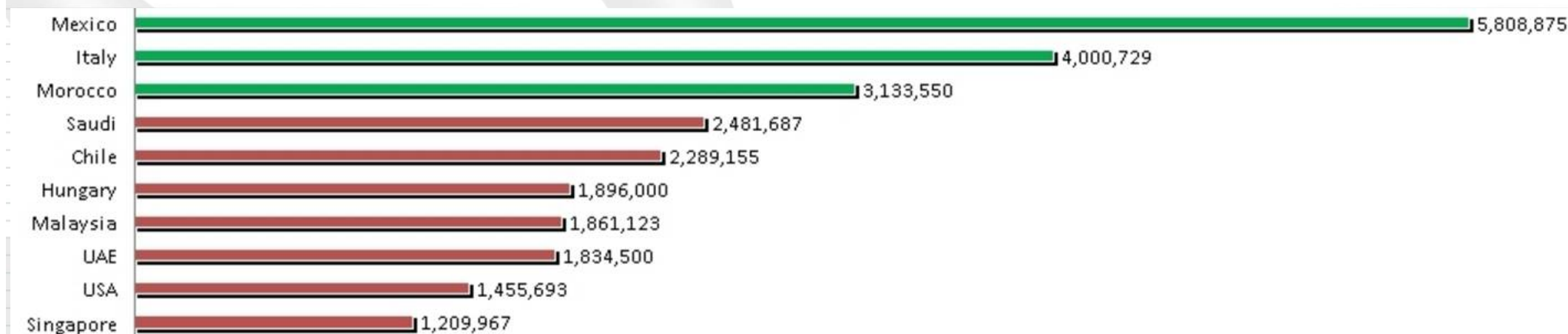


- 被公布的資料當然包含了買主的資料
 - 南韓陸軍、土耳其警察和美國FBI都是HackingTeam的熟客

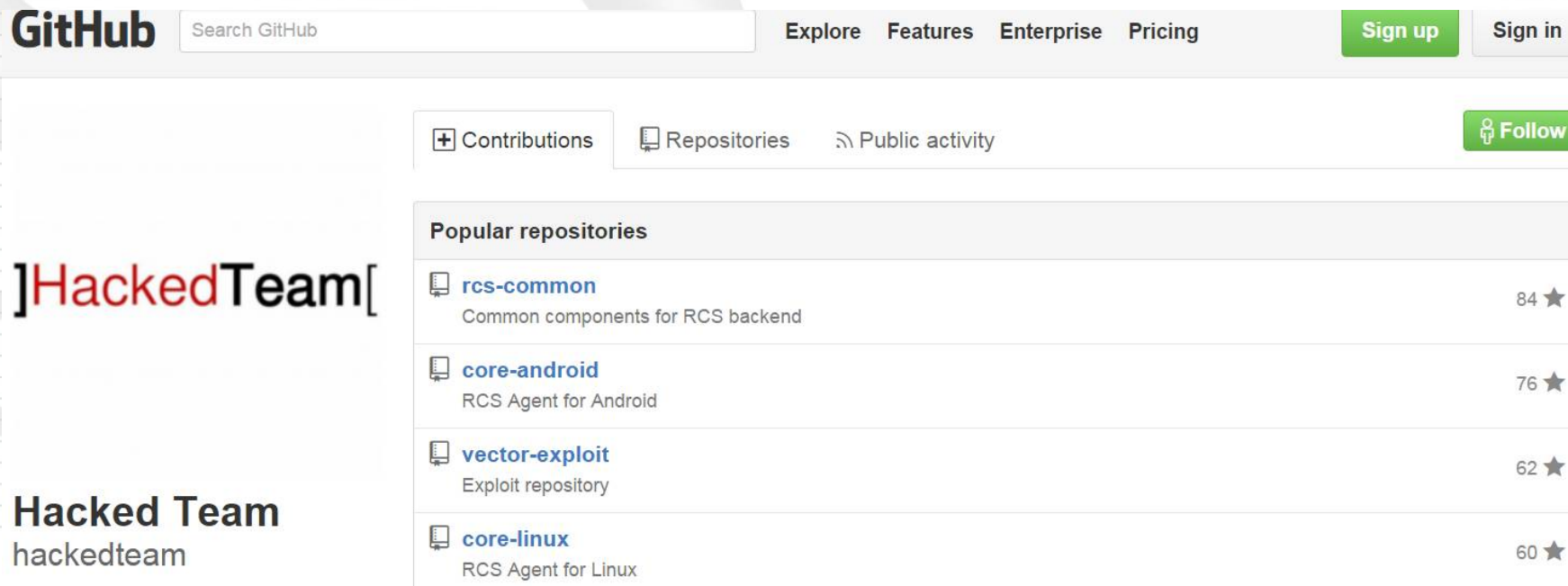
SKA	South Korea	The Army South Korea	12/31/2014	Active
NISS-01	Sudan	National Intelligence Security Service	12/31/2014	Not officially supported
THDOC	Thailand	Thai Police - Dep. Of Correctoin	7/31/2014	Expired
ATI	Tunisia	Tunisia (demo)	7/3/2011	Expired
TNP	Turkey	Turkish Police	11/10/2014	Active
MOI	UAE	Minister of Interior	12/31/2014	Active
UAEAF	UAE	UAE Air Force	5/31/2015	Active
DOD	USA	Dep.of Defence		Not Active
KATIE	USA	Drug Enforcement Agency	12/31/2014	Active
PHOEBE-PROD	USA	FBI - USA	6/30/2015	Active
NSS	Uzbekistan	National Security Service	1/31/2015	Active

- 不免俗的要來看一下那些政府最愛監聽

- 第一名：墨西哥(580萬美金)
- 第二名：義大利(400萬美金)
- 第三名：摩洛哥(313萬美金)



- 這駭客也一併把HackingTeam用的漏洞公布了
 - 3個Flash Zero-day漏洞
 - 3個Windows\IE Zero-day漏洞
 - 1個手機監控程式，可利用多個舊有漏洞自動植入
- 所有的漏洞以及程式都被上傳到Github



GitHub Search GitHub Explore Features Enterprise Pricing Sign up Sign in

Contributions Repositories Public activity Follow

Popular repositories

Repository Name	Description	Stars
<code>rcs-common</code>	Common components for RCS backend	84 ★
<code>core-android</code>	RCS Agent for Android	76 ★
<code>vector-exploit</code>	Exploit repository	62 ★
<code>core-linux</code>	RCS Agent for Linux	60 ★

[HackedTeam]

Hacked Team
hackedteam

- 此舉讓全世界的駭客都為之瘋狂
 - 一堆免費的Zero-day漏洞送你用
- 果不其然，隔沒幾天.....



- 發現各國都有相似的狀況
 - 追查社交工程郵件後，發現駭客的攻擊遍及東南亞(台灣、菲律賓、新加坡、馬來西亞、澳洲)等國，主要攻擊對象為政府機關以及與政府有關之民間組織



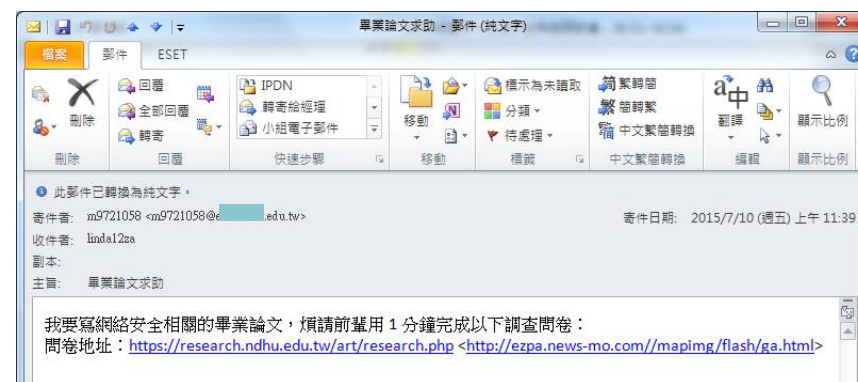
- 漏洞公布後應盡速進行修補
 - 以免遭駭客透過未修補之漏洞進行攻擊

7/5 義大利資安公司Hacking Team遭駭，該公司掌握之adobe零時差漏洞與後門程式原始碼外洩

7/8 adobe公司發佈修補程式



7/10中國駭客開始利用該漏洞製作惡意程式，透過社交工程方式攻擊政府機關



2015/7/5

2015/7/8

2015/7/10

- 趨勢探討

- APT依然是政府機關主要的資安威脅
- 複合式攻擊：Zero-day軟體漏洞+社交工程郵件

- APT攻擊案例分享

- 零時差弱點攻擊案例
- 網路設備被當中繼站案例
- Golden ticket案例
- 第三方程式案例

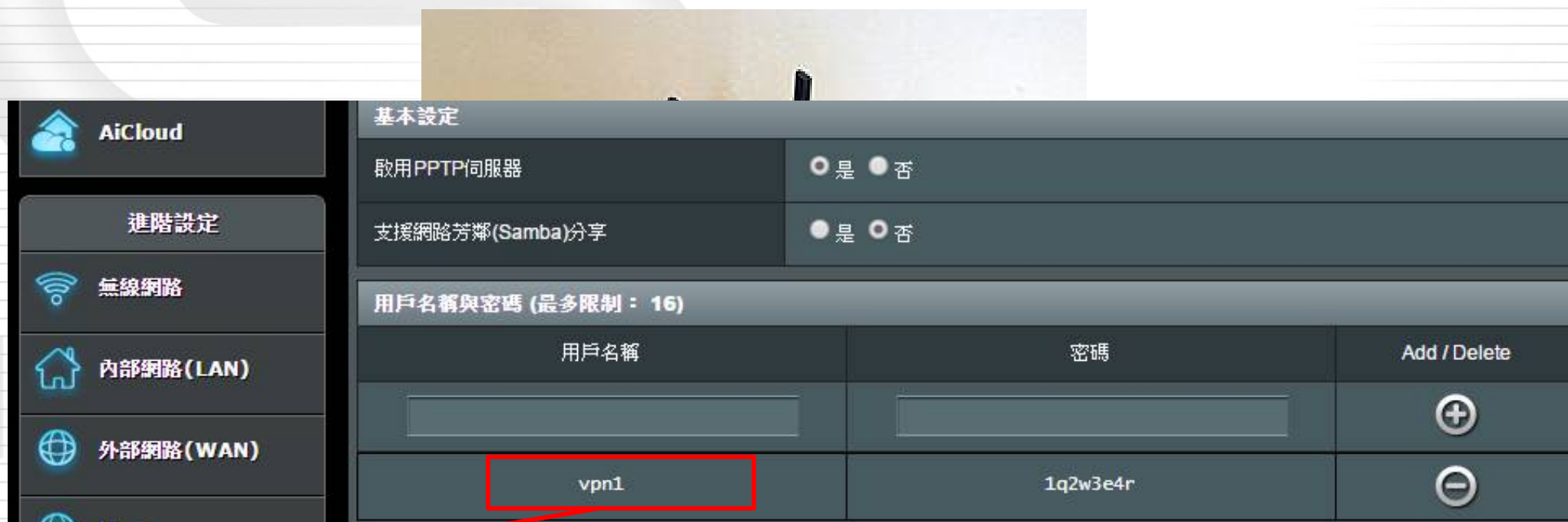
- 結論與建議

網路設備容易暴露在威脅中

- 網路設備管理不易，易遭駭客入侵
 - 因網路設備型號眾多，並無統一的管控方式與流程，加上設定上的疏忽，例如未使用高強度密碼，導致駭客輕易破解並入侵
 - 網路設備和電腦一樣會有漏洞存在，若原廠不願意釋出更新則難以抵禦駭客的攻擊
- 雖然入侵網路設備已不是新聞，但駭客至今仍不斷使用此類手法
 - 從2011年至今，每年均有駭客入侵網路設備並作為中繼站使用的紀錄

- 蒐集相關社交工程郵件並對其進行分析
 - 從信件附檔以及連結擷取相關惡意程式
 - 分析後發現一組駭客所使用的中繼站IP
- 追查中繼站IP後，發現該中繼站位於某民宅內
 - 但是該民宅主人表示，電腦未使用時都會關機，並非24小時運作
 - 但駭客通常都會選擇能24小時連線的電腦當中繼站使用

- 發現中繼站是一台無線分享器
 - 經過詳細調查後，發現中繼站是一台WiFi無線分享器，因未修改預設帳密，導致被駭客猜到密碼並入侵
 - 駭客入侵後即開啟分享器內建的VPN功能



駭客所建立的帳號

● 分享器自動轉送特定封包

- 檢視分享器中的其他設定，發現駭客將外部連入的所有80port與443port的封包傳送到192.168.10.2
- 192.168.10.2為VPN所配發的IP，因此只要駭客利用VPN連到分享器，便會持續收到受害者透過80port與443port送出的報到封包



內部網路 (LAN)



外部網路 (WAN)



IPv6



VPN 伺服器

虛擬伺服器清單 (最多限制：32)

服務名稱	通訊埠範圍	本地 IP	本地通訊埠	通訊協定	Add / Delete
				TCP	
https	443	192.168.10.2	443	TCP	
http	80	192.168.10.2	80	TCP	

- 從分享器LOG紀錄中發現駭客使用的紀錄
 - 檢視分享器的LOG，發現有外部IP(111.175.*.*)使用VPN的紀錄
 - 該外部IP所使用的VPN IP正巧是會收到轉送封包的192.168.10.2

```

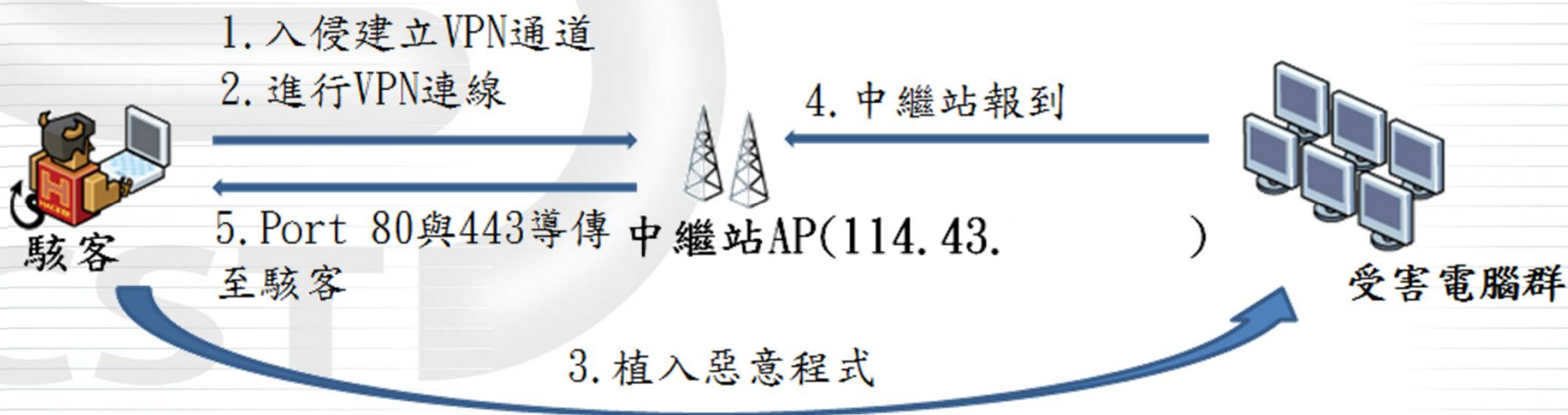
Jul 23 08:13:31 pptpd[3533]: CTRL: Starting call (launching pppd, opening GRE)
Jul 23 08:13:31 pptp[3534]: Plugin pptp.so loaded.
Jul 23 08:13:31 pptp[3534]: PPTP plugin version 0.8.5 compiled for pppd-2.4.5, linux-2.6.22.19
Jul 23 08:13:31 pptp[3534]: pppd 2.4.5 started by admin, uid 0
Jul 23 08:13:31 pptp[3534]: Using interface ppp10
Jul 23 08:13:31 pptp[3534]: Connect: ppp10 <--> pptp (111.175.    )
Jul 23 08:13:34 pptpd[3533]: CTRL: Ignored a SET LINK INFO packet with real ACCMs!
Jul 23 08:13:35 pptp[3534]: MPPC/MPPE 128-bit stateless compression enabled
Jul 23 08:13:35 pptp[3534]: Cannot determine ethernet address for proxy ARP
Jul 23 08:13:35 pptp[3534]: local IP address 192.168.1.1
Jul 23 08:13:35 pptp[3534]: remote IP address 192.168.10.2

```

駭客使用VPN的紀錄

駭客使用的VPN IP

- 該WiFi無線分享器被設定自動轉送封包
 - 只要駭客透過VPN連線至該分享器後，即可自動接收回傳的封包
 - 經追查後，發現受害的不只有台灣政府機關，還有美國、法國、英國、德國的IP連線至此中繼站



- 對機關內的所有網路設備進行安全控管
 - 需確實掌握機關內部所有網路設備
 - 定期檢視網路設備是否有安全性更新
 - 修改網路設備的預設密碼
 - 設定防火牆阻絕外部至網路設備的主動連線

- 趨勢探討

- APT依然是政府機關主要的資安威脅
- 複合式攻擊：Zero-day軟體漏洞+社交工程郵件

- APT攻擊案例分享

- 零時差弱點攻擊案例
- 網路設備被當中繼站案例
- Golden ticket案例
- 第三方程式案例

- 結論與建議

• LOG中出現異常的登入紀錄

- 某單位發現，該單位的特定使用者在內部AD上有異常登入紀錄(使用非該主機者帳號登入)，故請求協助檢測該主機



Mary的電腦

用Peter的帳號登入

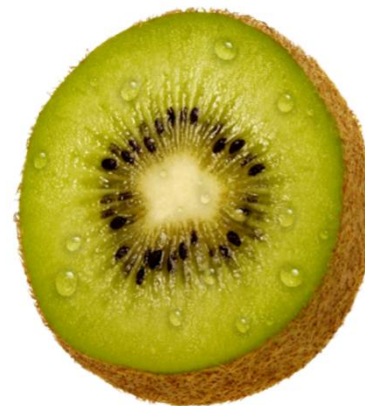


John的電腦

- 進行檢測後發現以下幾點
 - Mary的電腦兩年前已遭入侵並植入木馬程式
 - 由於使用了另外一位員工(Peter)的帳號，因此檢視Peter的電腦以及Domain Controller，但並未發現任何問題
 - 深入分析後，在Mary的電腦中發現了一個名為Mimikatz的駭客工具



Mary的電腦



Mimikatz



Pass-The-Ticket

- 駭客工具：Mimikatz

- 主要是用來進行Pass-The-Ticket攻擊

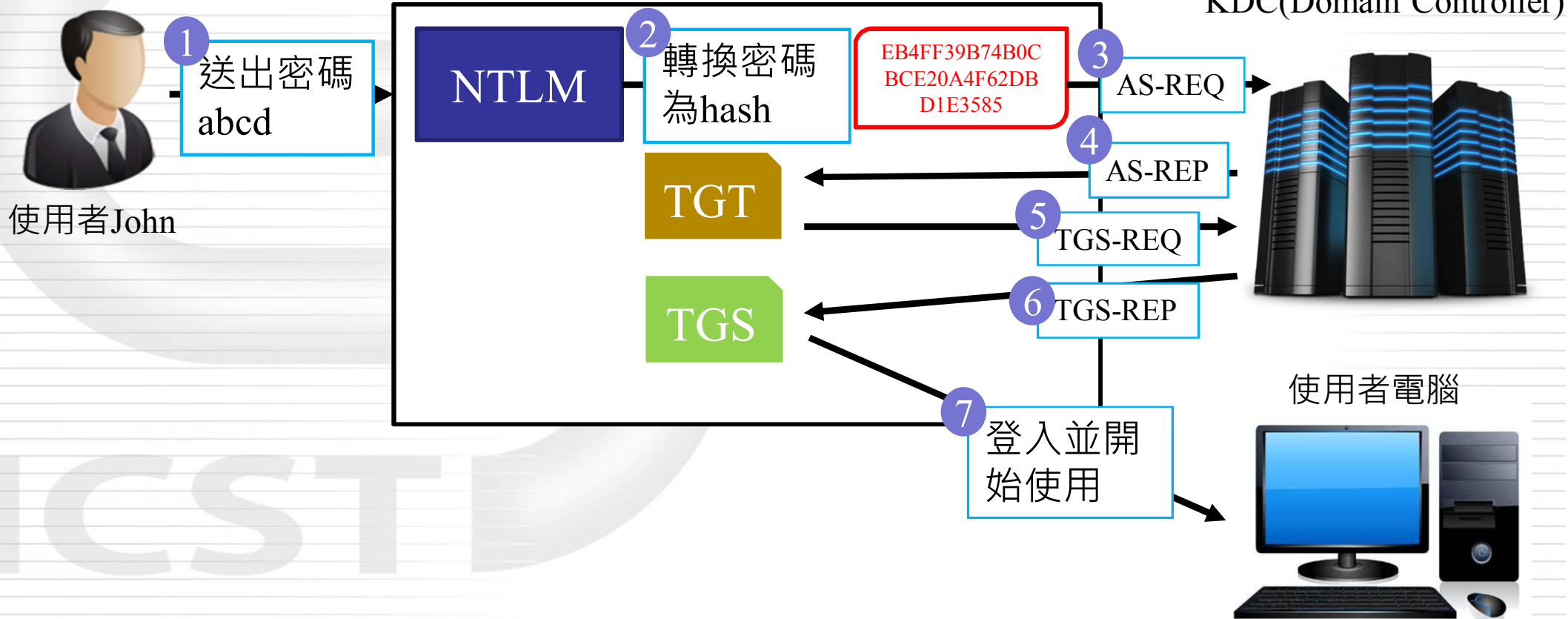
- Pass-The-Ticket攻擊

- 由於目前AD網域架構仰賴Kerberos進行驗證，而 Pass-The-Ticket攻擊即為針對此點進行攻擊，只要取得**TGT票證(Ticket Granting Ticket)**後便可以不用輸入密碼，並偽冒**當事人**進行登入
 - 使用者的TGT票證有效期限為10小時

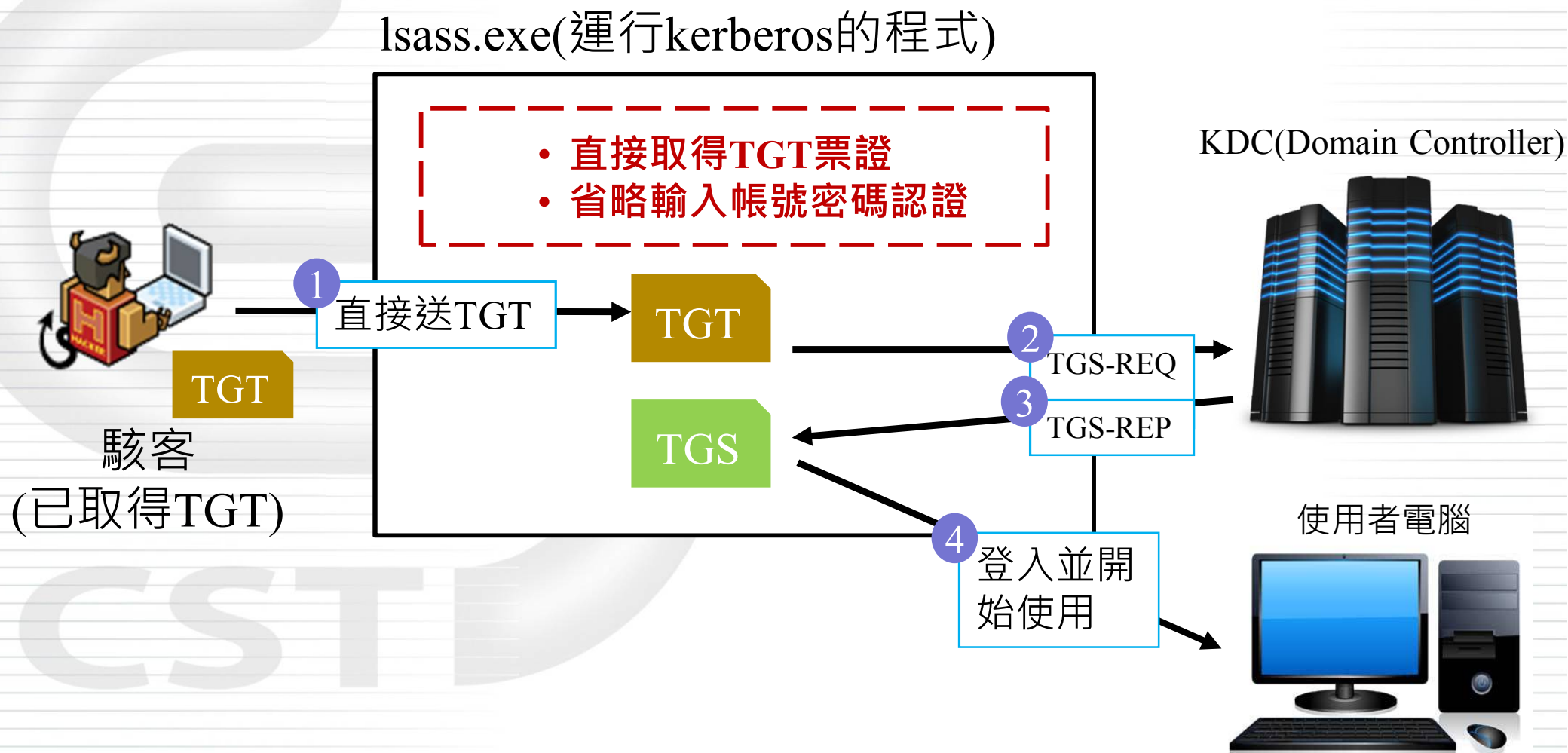


• 正常使用者驗證方式(with Active Directory)

lsass.exe(運行kerberos的程式)



● 使用Pass-The-Ticket的駭客驗證方式



- 利用系統TGT票證產生使用者票證
 - 除了各個使用者的TGT票證外，另有一個系統內建的TGT票證(即GoldenTicket)，系統TGT票證的功能是產生使用者的TGT票證，因此若駭客取得系統TGT票證後便可偽冒任何人進行登入
- GoldenTicket
 - 系統TGT票證儲存於krbtgt帳號的密碼欄位(NTLM hash)，此帳號為Active Domain安裝完成後自動建立的系統帳號
 - krbtgt帳號的密碼僅存放於Domain Controller中，欲取得須先入侵Domain Controller

- 駭客為何能擴散？

- 整個事件只有Mary的電腦遭入侵，其他台電腦都沒事
- 若需以此法擴散須先取得krbtgt帳號的密碼(NTLM hash)，為何密碼會洩漏出去？
 - 剛有提到krbtgt帳號的密碼(NTLM hash)只存在Domain Controller中

- 調查紀錄後發現，該單位兩年前曾被入侵

- 該單位在那次事件之後已經重灌Domain Controller、重新規劃網路架構、強化資安管控流程、採購新型資安防禦設備、購買SOC 24小時即時網路監控服務並強制所有使用者更改密碼
- 但是krbtgt的密碼沒有改，此密碼預設10年才會過期

● 可分析網域系統安全性日誌

– 1. 帳戶來源IP有誤(ID : 4624)

Type	Date	Time	Event	Source	Category
 Audit Success	2015/9/8	上午 07:36:43	4624	Microsoft-Windows-Sec	登入
Description 帳戶成功登入。 主旨： 安全性識別碼： S-1-0-0 帳戶名稱： - 帳戶網域： - 登入識別碼： 0x0 登入類型： 3 新登入： 安全性識別碼： S-1-5-21-705273604-3707611877-3454562850-1000 帳戶名稱： ART 帳戶網域： CSI 登入識別碼： 0xf557c13 登入 GUID： {A384AD8B-8955-6555-0B85-36A67A396DE7} 處理程序資訊： 處理程序識別碼： 0x0 處理程序名稱： - 網路資訊： 工作站名稱： - 來源網路位址： 192.168.124.2 來源連接埠： 49601					

該使用者所用的
電腦並非此IP

● 可分析本機或網域系統安全性日誌

– 2. 安全性識別碼與帳戶名稱不吻合(ID : 4624)

Type	Date	Time	Event	Source	Category
 Audit Success	2015/9/7	下午 05:53:37	4624	Microsoft-Windows-Sec	登入
 Audit Success	2015/9/7	下午 05:52:46	4624	Microsoft-Windows-Sec	登入

Description

帳戶成功登入。

主旨：

安全性識別碼：

S-1-0-0

帳戶名稱：

-

帳戶網域：

-

登入識別碼：

0x0

登入類型：

3

新登入：

安全性識別碼：

S-1-5-21-705273604-3707611877-3454562850-1111

帳戶名稱：

administrator

帳戶網域：

csi

登入識別碼：

0x2d654

登入 GUID：

{9375A84D-52B1-0F41-F682-06CA9EAD2E93}

Administrator的安全識別碼結尾應為50001111

Administrator的安全性識別碼結尾應為500而非1111

- 可分析本機或網域系統安全性日誌
 - 3. 帳戶網域有誤(ID : 4624、4672)

Type	Date	Time	Event	Source	Category
 Audit Success	2015/9/7	下午 05:04:41	4624	Microsoft-Windows-Sec	登入
Description 帳戶成功登入。 主旨： 安全性識別碼： S-1-0-0 帳戶名稱： - 帳戶網域： - 登入識別碼： 0x0 登入類型： 3 新登入： 安全性識別碼： S-1-5-21-705273604-3707611877-3454562850-500 帳戶名稱： administrator 帳戶網域： <3 eo.oe ~ ANSSI E> 登入識別碼： 0x5b185 登入 GUID： {D7E857AA-E29A-7FDD-E6E5-A672FED6B030}					

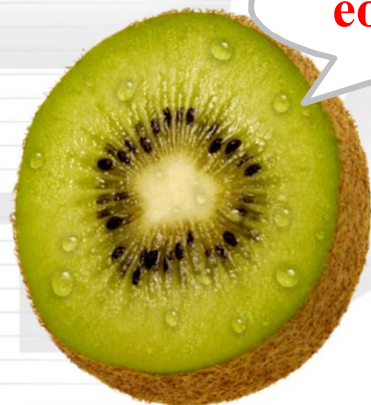
網域為奇怪的字串或 FQDN 或空白，應該要是網域縮寫

-----範例-----
 FQDN：abc.gov.tw
 網域縮寫：abc

- 可分析本機或網域系統安全性日誌

- 3. 帳戶網域有誤(ID：4624、4672)

- 由於Mimikatz有開放源碼，因此有許多不同版本，某些版本會在網域紀錄上留下不同的紀錄



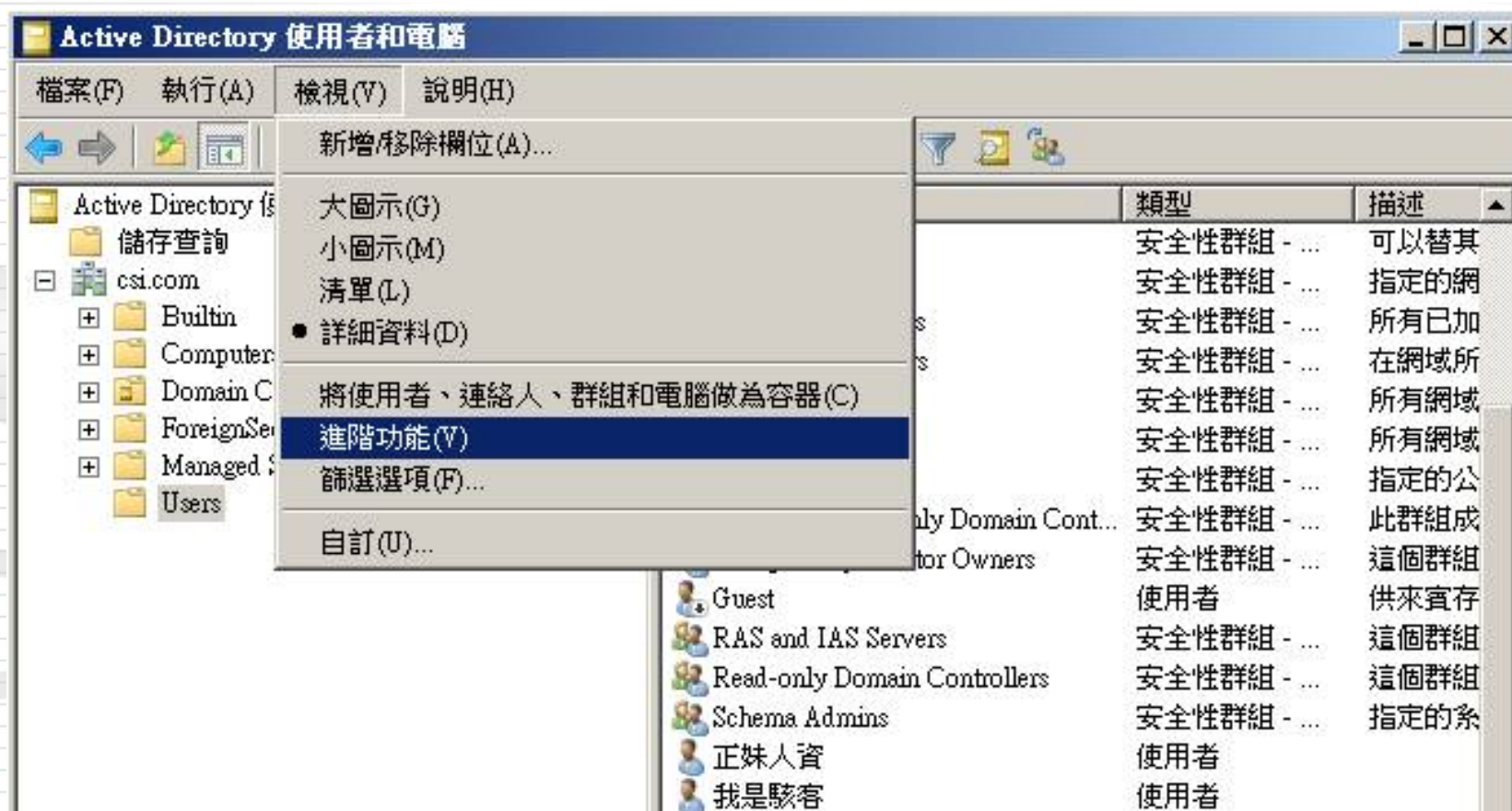
<3 eo.oe – ANSSI E>

eo.oe.kiwi :)



無紀錄

- 若確定已遭此手法攻擊，需修改krbtgt的密碼2次
 - 在Active Directory使用者和電腦的Users容器中可修改
 - 開啟「檢視」→「進階功能」



- 若確定已遭此手法攻擊，需修改krbtgt的密碼2次
 - 對帳號krbtgt按右鍵→「重設密碼」
 - 任意設一組高強度密碼，並於完成後重新開機



● 修改密碼後可能會出現錯誤(ID：4769)

- 若在網域系統安全性日誌中發現4769錯誤，且錯誤碼為0x1f時，代表有人嘗試用舊的hash登入，但登入失敗
- 改密碼後的10小時內有錯誤訊息是正常的

Type	Date	Time	Event	Source	Category
 Audit Failure	2015/11/11	下午 05:05:30	4769	Microsoft-Windows-Sec	Kerberos 服務票證操作
Description 已要求 Kerberos 服務票證。 帳戶資訊： 帳戶名稱： 帳戶網域： 登入 GUID：{00000000-0000-0000-0000-0000-0000-0000-0000-0000} 服務資訊： 服務名稱： 服務識別碼：S-1-0-0 網路資訊： 用戶端位址：::ffff:192.168.1.7 用戶端連接埠：52314 其他資訊： 票證選項：0x40810000 票證加密類型：0xffffffff 錯誤碼：0x1f 轉送的服務：-					

駭客使用192.168.1.7
的電腦欲進行擴散

0x1f表示駭客驗證失敗

- 趨勢探討

- APT依然是政府機關主要的資安威脅
- 複合式攻擊：Zero-day軟體漏洞+社交工程郵件

- APT攻擊案例分享

- 零時差弱點攻擊案例
- 網路設備被當中繼站案例
- Golden ticket案例
- 第三方程式案例

- 結論與建議

- 第三方程式(多用於網頁)

- 目前許多單位在架設網頁時都會採用第三方程式套件

- 此類的第三方程式通常有易用、免費、好上手等優點

- Apache、PHP、openssl、JBoss、Java Struts2、PhpMyAdmin、CkEditor.....等等

- 但這類第三方套件通常不易更新

- 不像Windows或Adobe系列會自行更新

APACHE
HTTP SERVER



CKEditor™

NEWS

Hackers exploit JBoss

iThome

新聞 產品評測 CIO DevOps 技術 專題 專欄 主題頻道 研討會 社群

新聞

OpenSSL重大漏洞Heartbleed 全球網路加密傳輸安全拉警報

iThome

新聞 產品評測 CIO DevOps 技術 專題 專欄 主題頻道 研討會 社群

Q搜尋

OpenSSL
使用

新聞

OpenSSL
1.0.1

Struts 2漏洞沒補好，Apache軟體基金會緊急重新釋出更新

ASF發現，今年3月2日釋出的Struts 2.3.16.1未能正確修補零時差攻擊漏洞，並於週日緊急釋出Struts 2.3.16.2。ASF強烈建議所有的開發人員進行版本更新。

文/ 陳曉莉 | 2014-04-29 發表

1.9 萬 按讚加入iThome粉絲團 12 6



圖片來源: 維基共享資源; 作者: U.S. Air Force photo/Capt. Carrie Kessler

iThome 電腦報
按讚追蹤 iThome 最新報導

1.9 萬

熱門新聞



最強大勒索軟體CryptoWall
進化到4.0版，更難偵測，連
檔名都加密！

2015-11-10



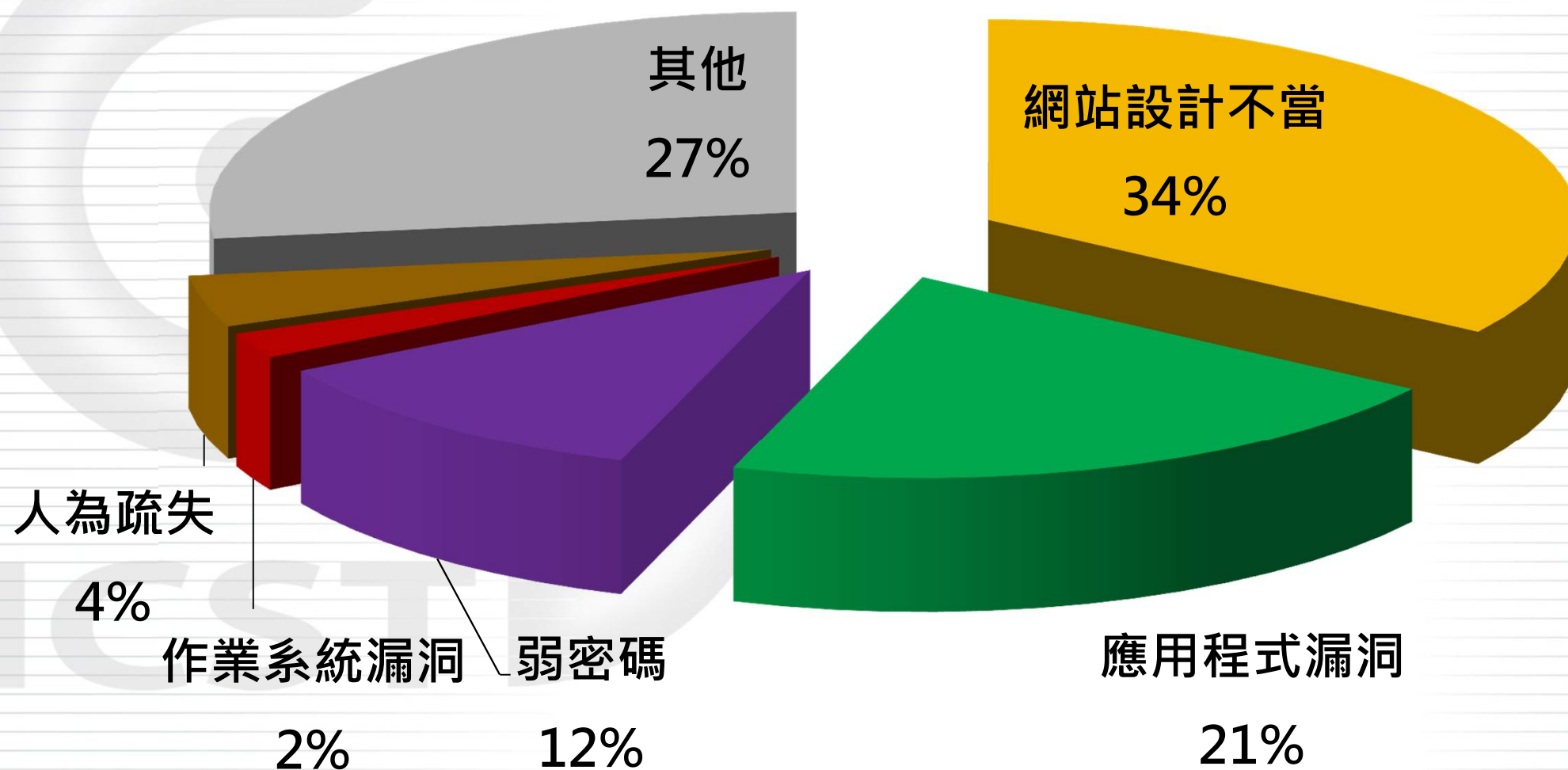
網管注意！勒索軟體已盯上
Linux網站！

2015-11-10



防毒軟體主管竟上社群網站大
爆顧客個資，日本F-Secure

- 原因大多為網站設計不當與應用程式漏洞



- 案例分享

- 技服中心收到某機關通報，該網站遭駭客入侵，希望可以協助進行事故調查

- 分析LOG後發現該網站已被駭客入侵2次

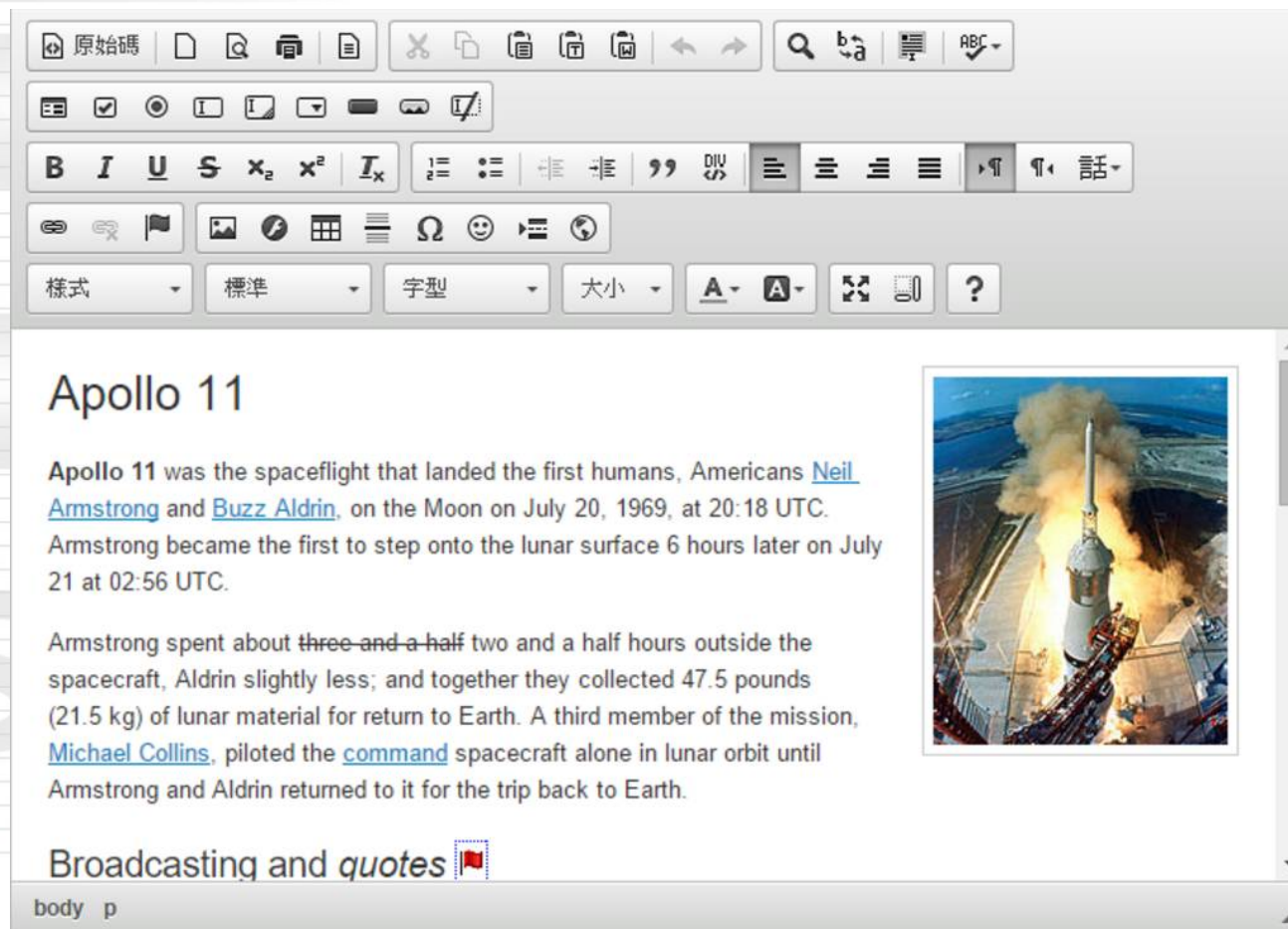
- 雖然該單位告知網頁後台有使用高強度之密碼保護，但因使用者的疏失，英文版的網頁後台並非為高強度密碼

- 英文版網頁後台採用CkEditor套件，可供駭客上傳網頁木馬

- 網站存在FckEditor套件的測試頁面，可供駭客上傳網頁木馬

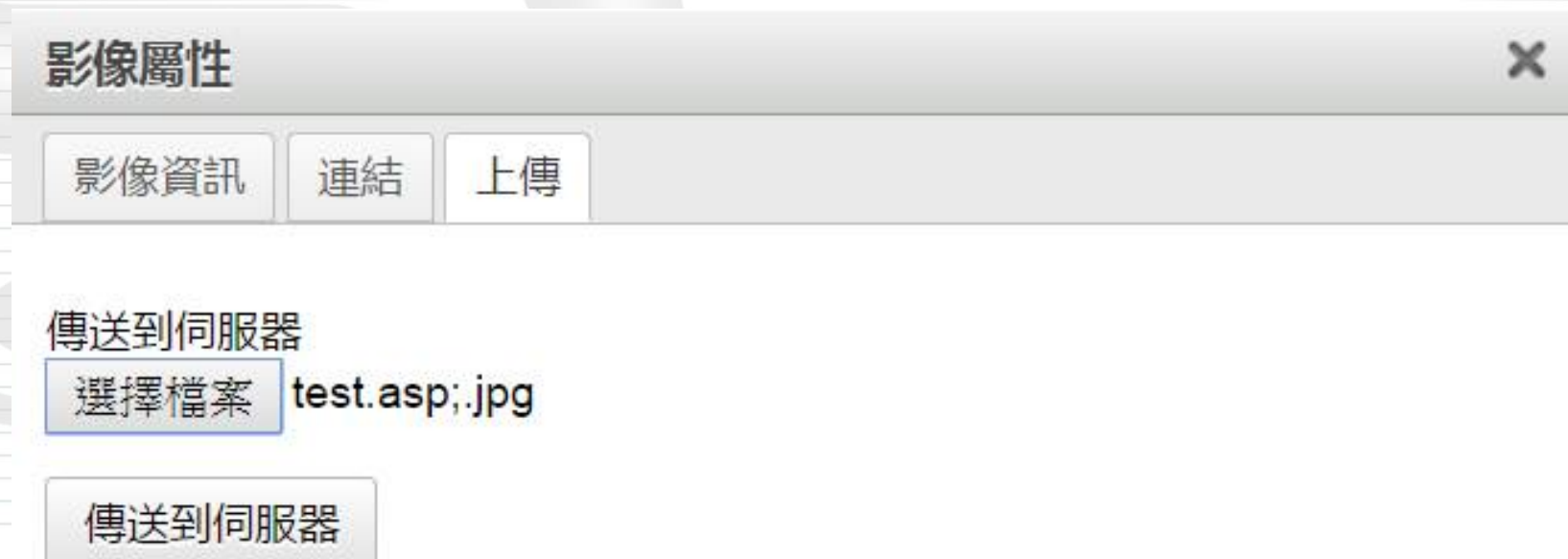
● CkEditor

- 常見的HTML編輯器，強調所見即所得，使用者可以輕易修改、維護網頁



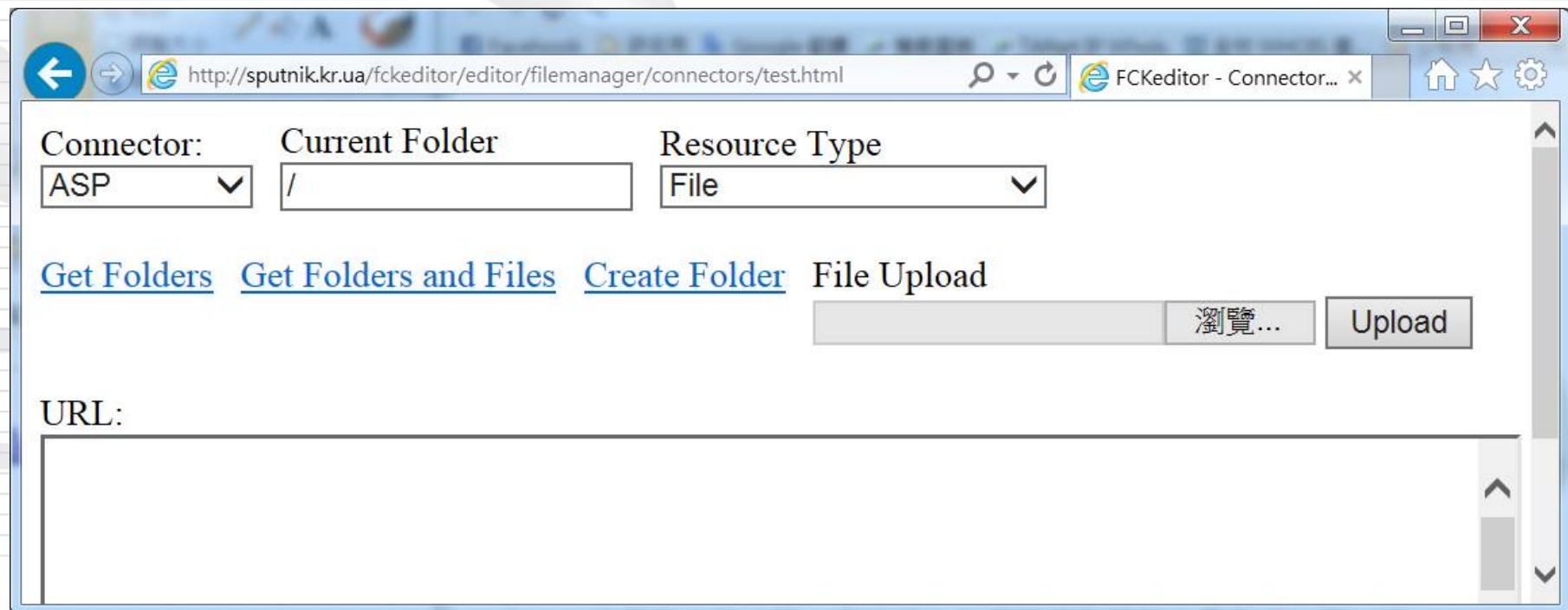
● CkEditor

- 此網頁位於後台，通過帳號密碼驗證後，即可指定需上傳的圖片
- 雖然僅可上傳圖片，但駭客可以把網頁木馬的名稱改為 **test.asp;.jpg** 即可順利上傳(CkEditor漏洞)，還可以順利執行(IIS6漏洞)



● FckEditor

- FckEditor為CkEditor的前身，外包廠商在測試網頁時，有使用到FckEditor套件，但卻未在完成測試後將其刪除
- 不過此網頁只有外包廠商知道，也沒有其他連結，所以機關完全不知道此測試網頁的存在



- 駭客怎麼會知道這網頁的存在？
 - 因為外包廠商用的是知名的第三方套件，因此駭客利用在google搜尋後台網頁就有連結了
 - 外包廠商為了方便測試，連帳號密碼驗證都省了，駭客找到連結就可以直接上傳木馬



- 網站管理管理要做好

- 所有帳號密碼須符合複雜度規範
- 若採用CkEditor等後台管理套件，需搭配帳號密碼的驗證機制
- 若有網站委外開發，需確認所有開發時所用的測試網頁均已刪除
- 可要求網頁委外廠商提供該網頁所使用的第三方程式清單，並定期檢視是否有更新

- Zero-Day漏洞雖難以防範，隨時更新軟體並注意社交郵件與可疑連結，仍可降低駭客入侵機率
- 網通設備應比照電腦主機套用較高規格之安全規範，避免成為資安的邊緣設備，成為駭客的溫床
- 應避免以遠端方式管理網域伺服器，降低管理者密碼外洩之可能，並定期變更具管理權帳之密碼
- 須確實掌握網站使用的各種套件，並定時執行弱點掃描與更新，以免遭駭客利用入侵

報告完畢
敬請指教