資通安全防護與案例分享

國立中央大學
桃園區域網路中心
技正 張二川

109年11月3日

自我介紹

- 中央警察大學
- 國立中央大學電子計算機中心
- 03-4227151
  - 分機57512
- center28@ncu.edu.tw

- ISO 27001:2013 LA
- PIMS LA
- CEH
- CHFI
- CCSK
- 技服中心資安職能
  - 網路架構與部署安全

大綱

- 資通安全法簡介
- 案例分享與防護作為
- 社交工程
- 資安好習慣
- Kahoot !
- Q & A

資通安全法簡介

- 107年5月經立法院三讀通過「資通安全管理法」，6月6日經總統公布，108年1月1日實施。
  - 資通安全管理法施行細則
  - 資通安全責任等級分級辦法
  - 資通安全事件通報及應變辦法
  - 特定非公務機關資通安全維護計畫實施情形稽核辦法
  - 資通安全情資分享辦法
  - 公務機關所屬人員資通安全事項獎懲辦法
- 資通安全管理法制化，有效管理資通安全風險，以建構安全完善的數位環境

※ 資通安全管理法之簡介與因應， 資訊工業策進會科技法律研究所， https://stli.iii.org.tw/article-detail.aspx?no=0&tp=3&i=79&d=8259 （最後瀏覽日：2020/10/20）

資通安全責任等級 C級應辦事項

附表五 資通安全責任等級 C 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。

資通安全責任等級 C級應辦事項

技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

資通安全責任等級 C級應辦事項

認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少一名人員接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	資通安全專職人員總計應持有一張以上。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有一張以上，並持續維持證書之有效性。

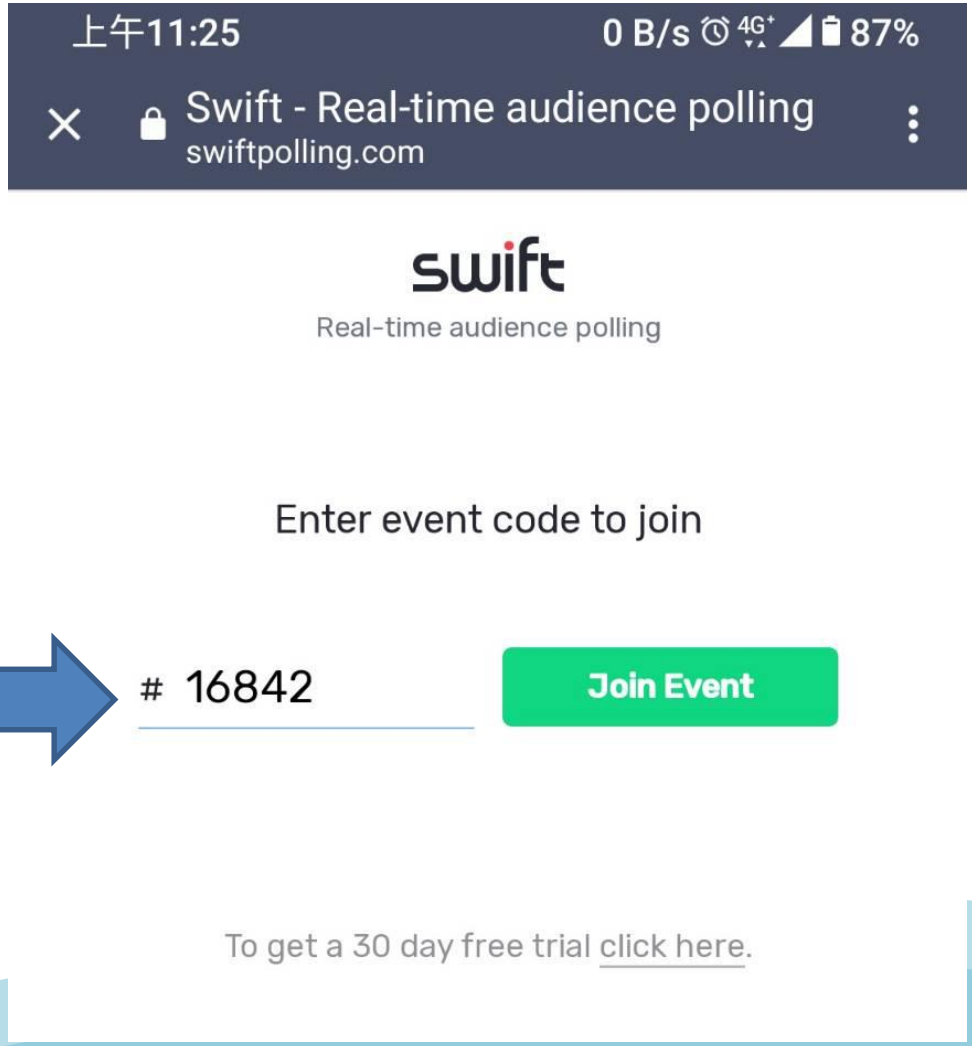
資通安全責任等級D級應辦事項

附表七 資通安全責任等級D級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

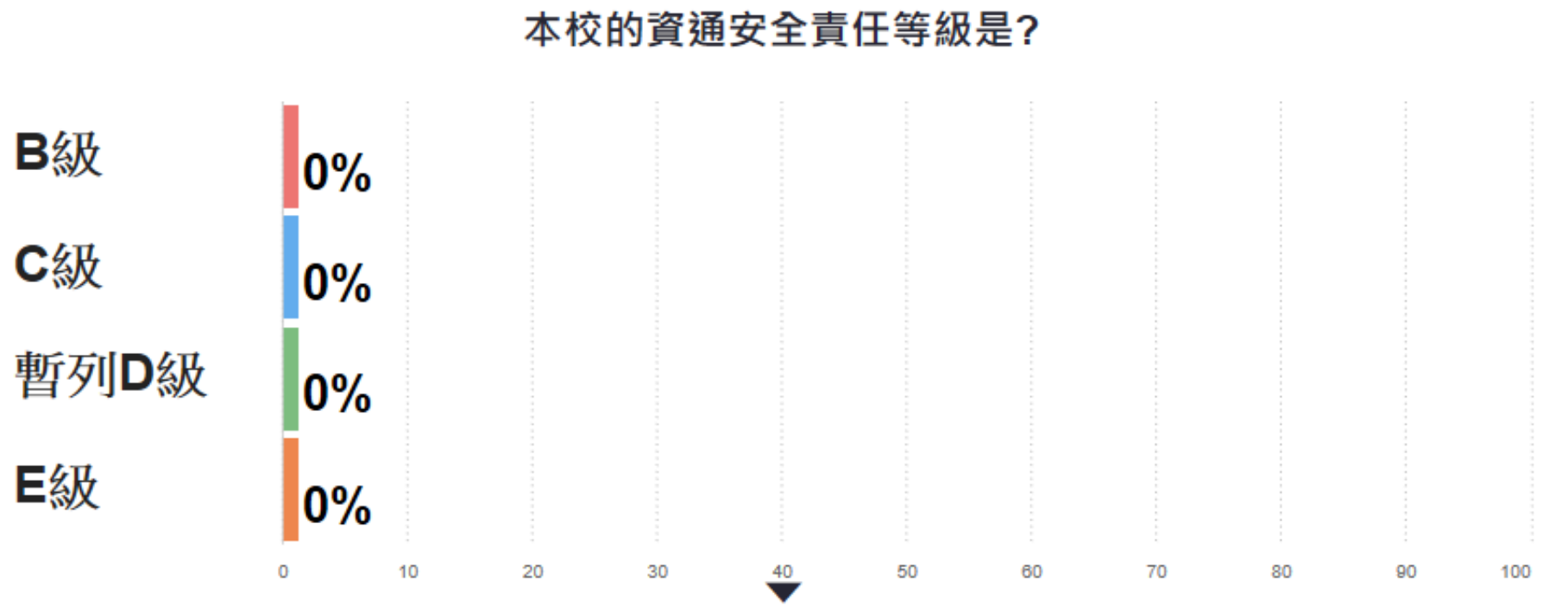
Go to **swiftpolling.com** & enter **16842**



輸入 16842

本校的資通安全責任等級是?

Go to **swiftpolling.com** & enter **16842**



This poll is inactive, click Start to activate poll

您覺得資安問題會發生在什麼地方?

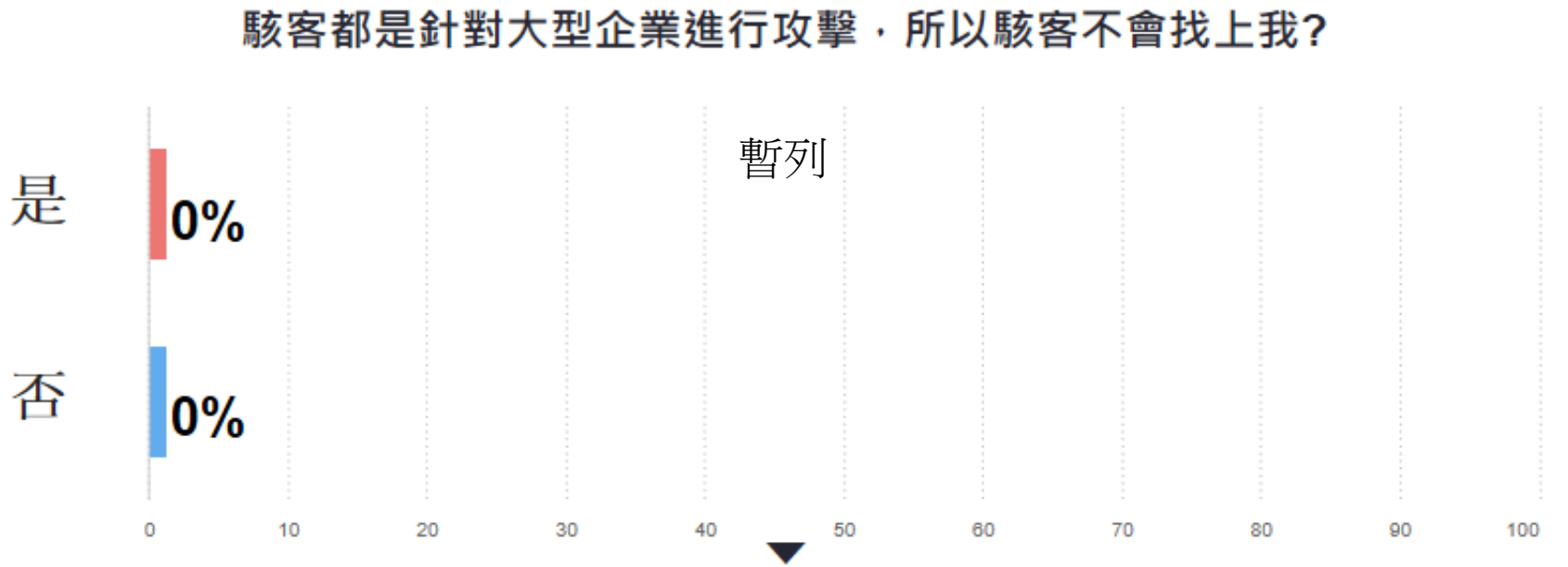
近期大型資安事件

- 台積電遭病毒攻擊　損失76億、報廢上萬片晶圓
- 一銀ATM遭駭事件大剖析
- 全球散播最廣、「最會裝」的木馬！Emotet 最近又偽裝成 Windows 更新
- 伊朗APT駭客組織鎖定全球12所大學發動網路釣魚攻擊
- 臺灣史上第一次券商集體遭DDoS攻擊勒索事件
- Garmin證實遭駭客勒索軟體攻擊
- 層出不窮的資安攻擊

- 104 人力銀行 592萬 筆個資在中國「暗網交易論壇」出售
- 繼 104 人力銀行之後。另一家 1111 人力銀行也在相同的中國「暗網交易論壇」被出售 335萬 筆個資

駭客都是針對大型企業進行攻擊，所以駭客不會找上我?

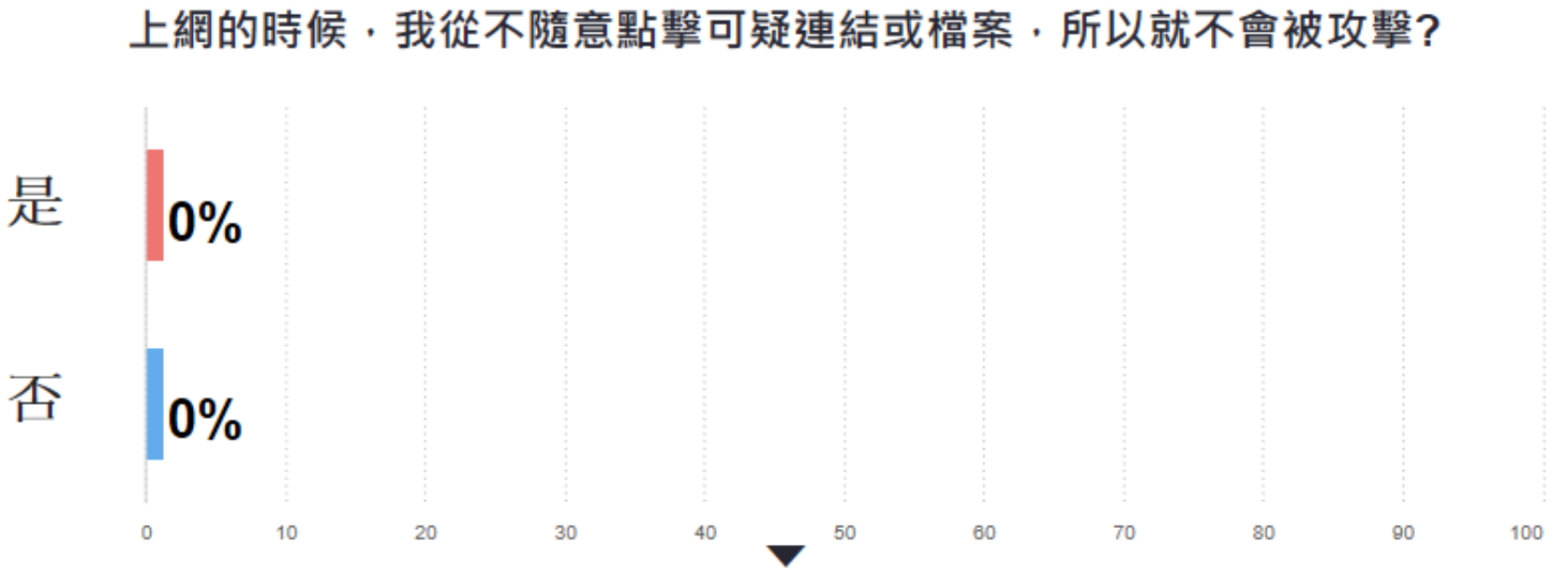
Go to **swiftpolling.com** & enter **16842**



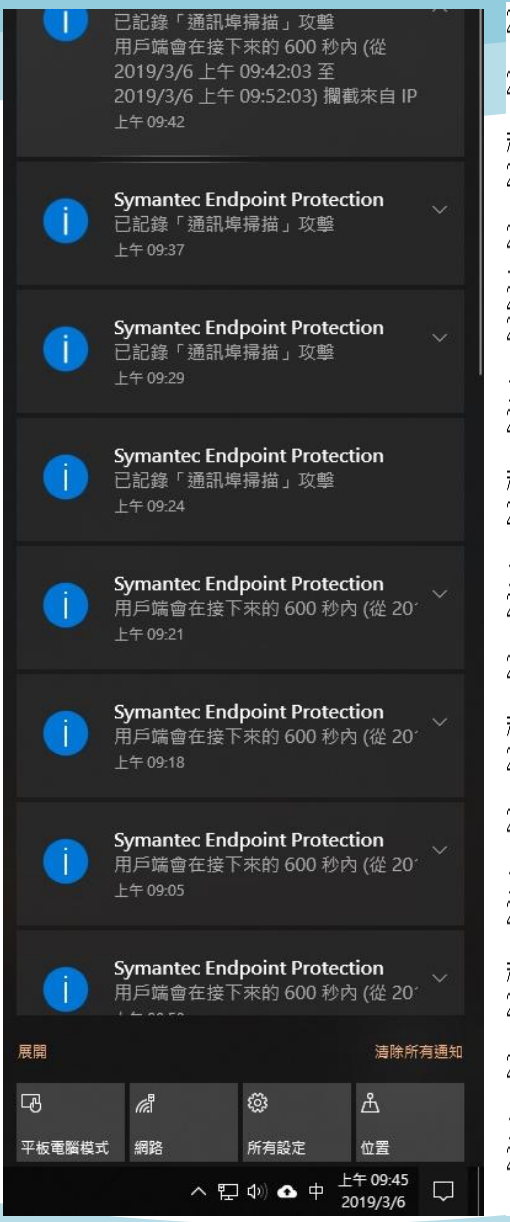
This poll is inactive, click Start to activate poll

上網的時候，我從不隨意點擊可疑連結或檔案，所以就不會被攻擊?

Go to **swiftpolling.com** & enter **16842**



This poll is inactive, click Start to activate poll



243 2019/3/4 上午 08:31:27 通訊埠掃描 次要 內送 TCP 185.153.196.85 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:28:16 2019/3/4 上午 08:30:25 有人正在掃描您的電腦。

244 2019/3/4 上午 08:31:27 主動回應 主要 內送 無 185.153.197.61 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:31:24 2019/3/4 上午 08:41:24 用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:31:24 至 2019/3/4 上午 08:41:24) 攔截來自 IP 位址 185.153.197.61 的流量。

245 2019/3/4 上午 08:32:28 通訊埠掃描 次要 內送 TCP 185.153.197.61 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:28:18 2019/3/4 上午 08:31:24 有人正在掃描您的電腦。

246 2019/3/4 上午 08:33:42 已接受執行檔變更 資訊 外寄 UDP 239.255.255.250 0 01-00-5E-7F-FF-FA 140.115.184.100 0 88-D7-F6-54-93
-8F C:\Program Files (x86)\Google\Chrome\Application\chrome.exe ncudarren NCUDARREN Default 1
2019/3/4 上午 08:32:40 2019/3/4 上午 08:32:40 應用程式在您上次開啟之後已變更，程序 ID: 9768

247 2019/3/4 上午 08:41:28 已斷開主動回應 資訊 無 無 185.153.196.85 0 N/A 140.115.184.100 0 N/A
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:40:26 2019/3/4 上午 08:40:26 解除始於 2019/3/4 上午 08:30:26 的「主動回應」。IP 位址
185.153.196.85 的流量攔截持續時間為 600 秒。

248 2019/3/4 上午 08:42:24 主動回應 主要 內送 無 185.153.196.85 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:42:18 2019/3/4 上午 08:52:18 用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:42:18 至 2019/3/4 上午 08:52:18) 攔截來自 IP 位址 185.153.196.85 的流量。

249 2019/3/4 上午 08:42:29 已斷開主動回應 資訊 無 無 185.153.197.61 0 N/A 140.115.184.100 0 N/A
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:41:25 2019/3/4 上午 08:41:25 解除始於 2019/3/4 上午 08:31:24 的「主動回應」。IP 位址
185.153.197.61 的流量攔截持續時間為 600 秒。

250 2019/3/4 上午 08:43:19 通訊埠掃描 次要 內送 TCP 185.153.196.85 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:41:05 2019/3/4 上午 08:42:18 有人正在掃描您的電腦。

251 2019/3/4 上午 08:44:21 主動回應 主要 內送 無 185.153.197.61 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:44:18 2019/3/4 上午 08:54:18 用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:44:18 至 2019/3/4 上午 08:54:18) 攔截來自 IP 位址 185.153.197.61 的流量。

252 2019/3/4 上午 08:45:22 通訊埠掃描 次要 內送 TCP 185.153.197.61 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:41:49 2019/3/4 上午 08:44:18 有人正在掃描您的電腦。

253 2019/3/4 上午 08:53:23 已斷開主動回應 資訊 無 無 185.153.196.85 0 N/A 140.115.184.100 0 N/A
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:52:19 2019/3/4 上午 08:52:19 解除始於 2019/3/4 上午 08:42:18 的「主動回應」。IP 位址
185.153.196.85 的流量攔截持續時間為 600 秒。

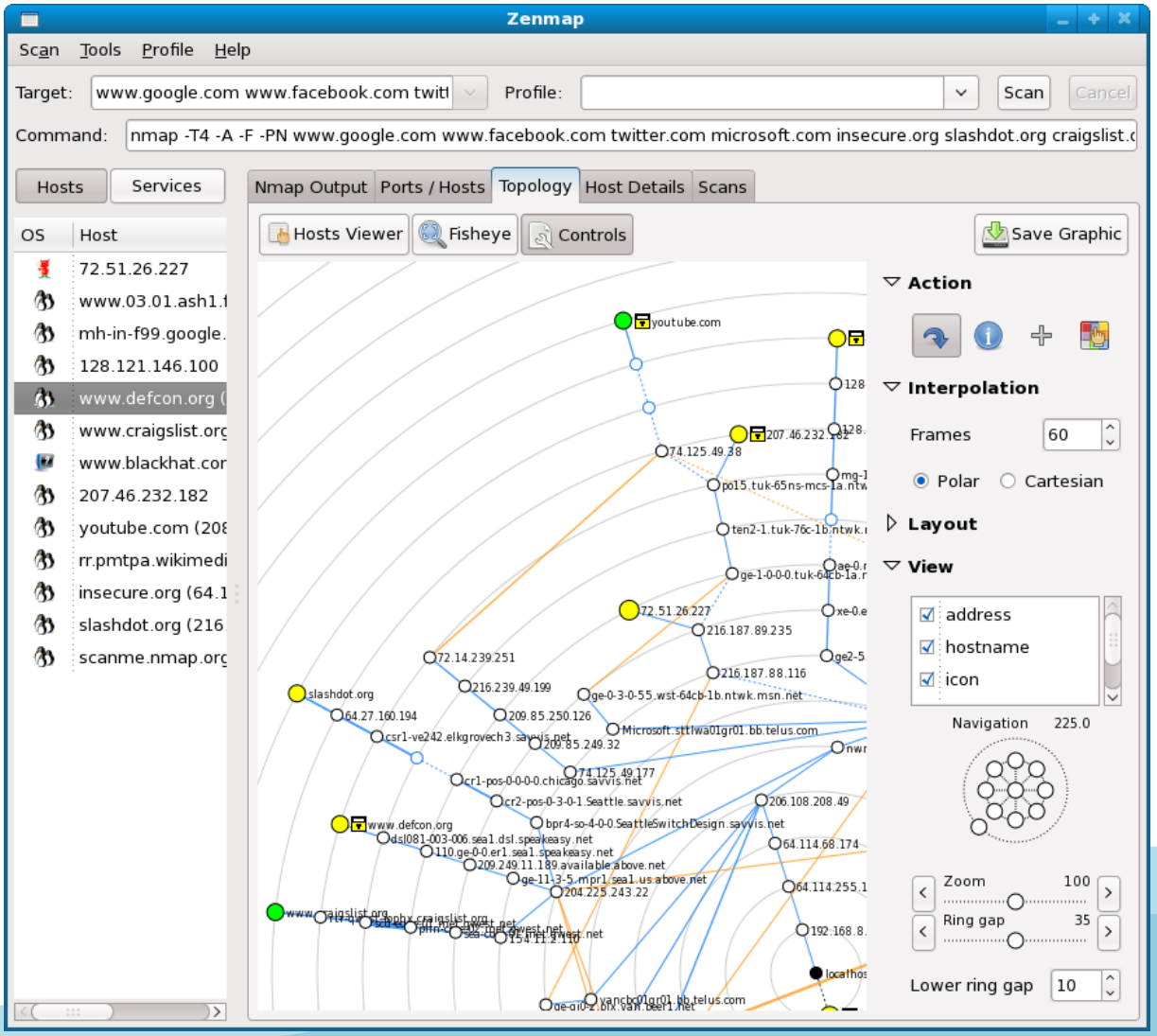
254 2019/3/4 上午 08:53:59 主動回應 主要 內送 無 185.153.196.85 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:53:58 2019/3/4 上午 09:03:58 用戶端會在接下來的 600
秒內 (從 2019/3/4 上午 08:53:58 至 2019/3/4 上午 09:03:58) 攔截來自 IP 位址 185.153.196.85 的流量。

255 2019/3/4 上午 08:54:58 通訊埠掃描 次要 內送 TCP 185.153.196.85 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:52:38 2019/3/4 上午 08:53:57 有人正在掃描您的電腦。

256 2019/3/4 上午 08:55:19 已斷開主動回應 資訊 無 無 185.153.197.61 0 N/A 140.115.184.100 0 N/A
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:54:19 2019/3/4 上午 08:54:19 解除始於 2019/3/4 上午 08:44:18 的「主動回應」。IP 位址
185.153.197.61 的流量攔截持續時間為 600 秒。

257 2019/3/4 上午 08:57:22 主動回應 主要 內送 無 185.153.197.61 0 64-A0-E7-40-88-41 140.115.184.100 0 88-D7-F6-54-93-8F
ncudarren NCUDARREN Default 1 2019/3/4 上午 08:57:22 2019/3/4 上午 09:07:22 用戶端會在接下來的 600

連上網際網路的那一刻起，即有人不停掃描、攻擊你的裝置




只要我不上網
就不會遭受資
訊安全威脅?

IoT設備

- 駭客架站即時轉播全球上萬台網路攝影機，私密生活全都露
- http://www.insecam.org/cn/bycountry/TW/
- http://www.insecam.org/cn/view/832450/
- http://www.insecam.org/cn/view/812140/

- IoT設備的預設密碼
- 韌體修補

http://www.insecam.org/cn/bycountry/TW/?page=1

僵屍網路-Botnet

- 利用惡意程式控制網路上的設備，這些殭屍電腦網路在 C2 端（也就是控制者）的命令下統一行動，就組成了殭屍網路。
- 惡意殭屍程式在全網進行掃描，一旦發現有漏洞的設備（電腦、硬體等）就馬上入侵控制，再以新的殭屍設備為跳板，繼續感染其他設備。
- 這些殭屍大軍，少則有幾千台設備，多則達到數百萬台設備
- 圖書館LED燈控制器的IP位址成攻擊跳板，駭客用來散布惡意程式的，竟然是一個不起眼的圖書館LED燈控制裝置
- 發動DDOS、發送垃圾郵件、竊取秘密、濫用資源

https://technews.tw/2020/03/13/microsoft-disrupts-a-botnet-that-infected-9-million-computers/

挖礦

第一個計算出正確雜湊碼的礦工 ，就可以獲得一定單位的貨幣作為報酬。 新聞

- 網頁
- 惡意程式
- OCAM
- 手機

勒索軟體


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (traditiona
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪到你，就要看您的運氣怎麼樣了。
Payment will be raised on
5/18/2017 08:43:45
Time Left
02:23:58:54
Your files will be lost on
5/22/2017 08:43:45
Time Left
06:23:58:54
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt
azofreeware.com

備份三二一原則

- 重要檔案至少備份三份
- 使用兩種不同形式存放檔案
- 其中一份備份要存放異地

https://blog.trendmicro.com.tw/?p=4707

你還在用Flash Player嗎

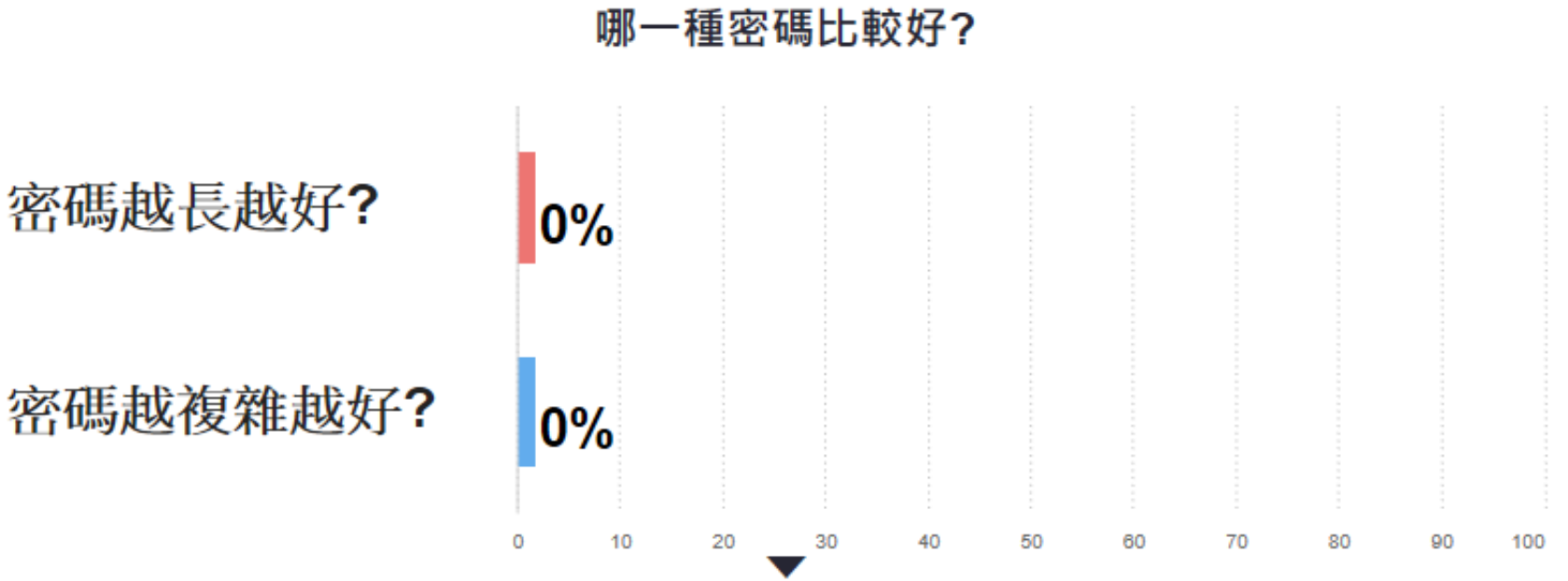
- 長期而言，由於漏洞過多，加上HTML5、WebGL及WebAssembly標準成熟，功能足以取代，Adobe自己也不鼓勵使用者繼續使用Flash Player。Adobe宣布在今年底正式終止Flash Player的更新及發行。

- 位於Flash Player的漏洞CVE-2020-9746，能在使用者造訪網站時，利用網站的HTTP回應插入惡意字串加以觸發，成功開採可能造成應用程式當掉，引發遠端程式碼執行。

https://www.ithome.com.tw/news/140517

哪一種密碼比較好?

Go to **swiftpolling.com** & enter **16842**



This poll is inactive, click Start to activate poll

密碼

- 密碼內容越複雜越好?
- 密碼長度越長越好?
- 測試密碼強度的網站安全嗎?
- 你的帳號是否都用同一組密碼?

密碼產生器/密碼強度檢測器

密碼產生器可以建立隨機密碼，為您所有帳號建立強式密碼，讓其他人幾乎不可能猜到它們。

密碼檢測器測試您的密碼安全強度，協助您保持安全。

密碼產生器 | 密碼強度檢測器

測試您的密碼強度		建立強式密碼條件
輸入密碼： Password:	•••••	長度最少需要 8 位字符 Minimum 8 characters in length 必須含有以下3/4先決條件： Contains 3/4 of the following items: - 大寫英文字 Uppercase Letters - 小寫英文字 Lowercase Letters - 數字 Numbers - 特殊符號 Symbols
隱藏/顯示： Hide/Display:	☑	
密碼強度數值： Score:	44%	
密碼優勢： Complexity:	好	

加分條件		改變條件	計算公式	複數	積分
✗	密碼總字數 Number of Characters	輸入 Flat	+(次數*4) +(n*4)	5	+ 20
✓	大寫英文字母數 Uppercase Letters	條件/改變 Cond/Incr	+((長度-次數)*2) +((len-n)*2)	1	+ 8
✓	小寫英文字母數 Lowercase Letters	條件/改變 Cond/Incr	+((長度-次數)*2) +((len-n)*2)	2	+ 6
✓	數字出現次數 Numbers	條件 Cond	+(次數*4) +(n*4)	1	+ 4
✓	特殊符號個數 Symbols	輸入 Flat	+(次數*6) +(n*6)	1	+ 6
✓	密碼的中間部份出現數字或符號 Middle Numbers or Symbols	輸入 Flat	+(次數*2) +(n*2)	1	+ 2
✗	達到最低需求 Requirements	輸入 Flat	+(次數*2) +(n*2)	4	0

誰在追蹤你的數位足跡

- 在網路上的行為所留下的紀錄與軌跡，正是你的數位足跡
- 網站上的留言、發表的文章、上傳的照片或影片、瀏覽過的網站、搜尋過的關鍵字，以及社群網站上的朋友。
- 廠商可以參考你輸入到搜尋引擎中的關鍵字，向你推銷你可能會有興趣的相關特定產品服務。
- 使用Chrome展示

https://isafe.moe.edu.tw/article/1958?user_type=4&topic=8

Google Hacking

- 利用google搜尋功能，從網路中找尋機敏資料
- 機敏資訊：如名冊、身分證字號、曾經被找到的漏洞網頁或原始碼
- 使用方法：點選所列出的"關鍵字"網址
- https://www.google.com.tw/search?q=intext:%22powered+by+webcamXP+5%22&gws_rd=cr&ei=wkkdWPGlHIvG0gTVrbqwBg
- https://www.exploit-db.com/google-hacking-database

你裝的APP 安全嗎?

行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0083	發布時間	Thu Aug 13 09:36:35 CST 2020
事件類型	其他	發現時間	Tue Aug 11 00:00:00 CST 2020
警訊名稱	部分應用程式存在資安疑慮，請避免於公務手機與電腦中安裝使用		
內容說明	據外媒報導，抖音(TikTok)與微信(WeChat)應用程式存在資安疑慮，可能蒐集使用者資訊並回傳至特定伺服器，請避免於公務手機與電腦中安裝與使用抖音與微信等應用程式。		
影響平台	行動裝置與個人電腦		
影響等級	中		
建議措施	1. 避免在公務手機與電腦中安裝抖音或微信等有資安疑慮之應用程式 2. 避免於有資安疑慮之應用程式中討論與傳遞公務資料		
參考資料	1. https://www.darkreading.com/risk/us-lawmakers-fear-chinese-owned-tiktok-poses-security-risk/d/d-id/1336188 2. https://www.reuters.com/article/us-usa-china-apps-pompeo/u-s-steps-up-campaign-to-purge-untrusted-chinese-apps-idUSKCN2512YO		

社交工程

- 社交工程 (Social Engineering) 係利用人性弱點，運用簡單的溝通和欺騙技倆，以獲取帳號、通行碼、身分證號碼或其他機敏資料，來突破單位的資通安全防護，進行非法的存取、破壞行為。

- 「社交工程」，就是詐騙

- 駭客思維：可以簡單，何必複雜

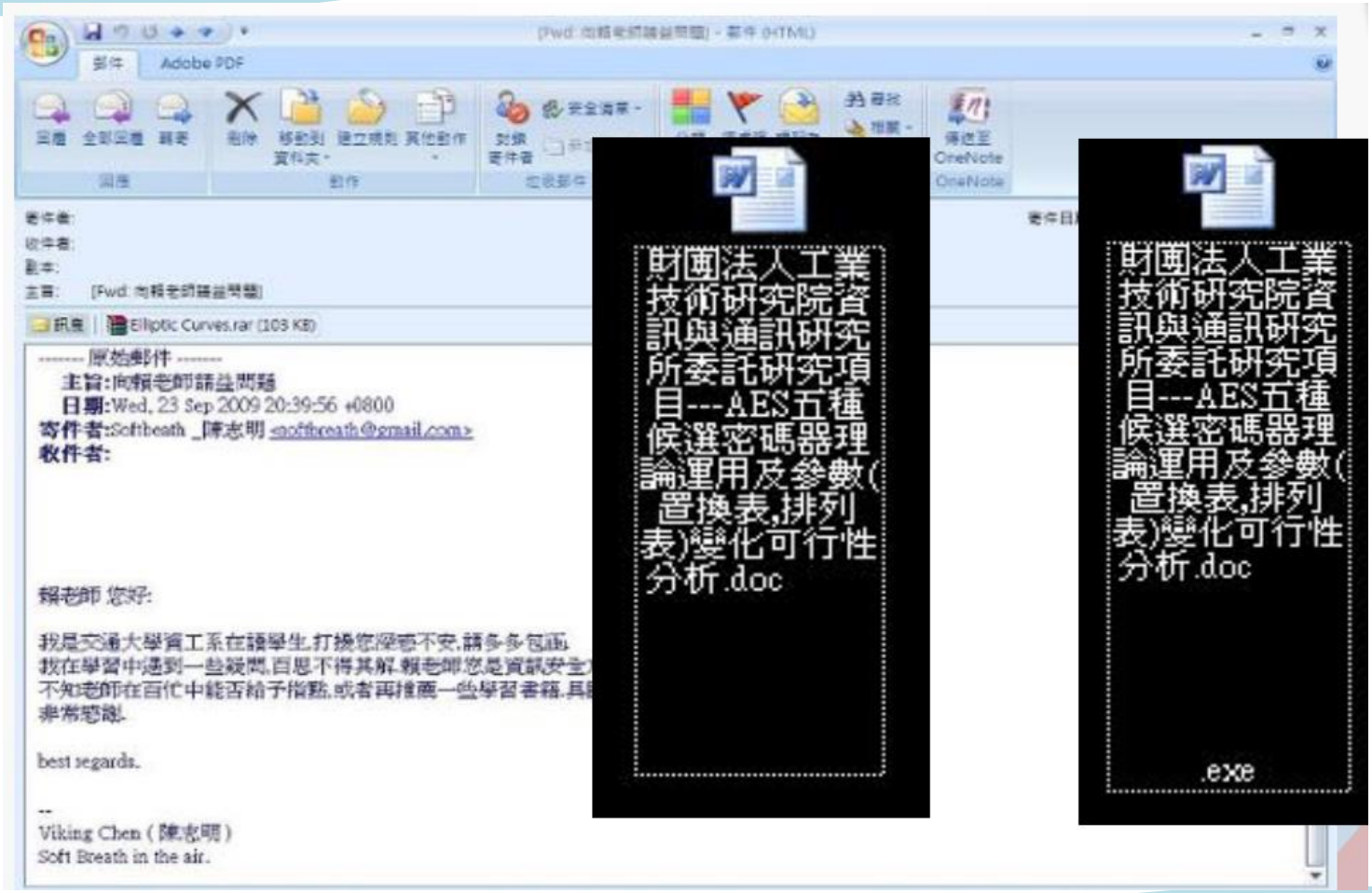
社交工程

- 社交工程電子郵件
- 電話詐騙
- 網路釣魚 🔗
- 圖片、檔案內含惡意程式
- 誘騙執行程式(副檔名)
- 惡意連結

電子郵件預覽功能一定要關閉

網路釣魚（Phishing）就是網路犯罪份子通過偽造的電子郵件或是網站來誘騙你的個人資料，像是帳號名稱和密碼。

檔案副檔名



- 另外展示RLO實例

- 惡意檔案檢測服務
  - https://viruscheck.tw/
- 芬-安全雲端病毒檢測系統 - Submit A Sample
  - https://www.f-secure.com/en/business/support-and-downloads/submit-a-sample#sample-file
- Windows Sandbox

資安好習慣

1.不明人士要盤查

2.社交工程要小心

3.電腦不用要登出

4.精密文件要保護

5.密碼設定要穩固

6.重要資料要備份

7.電腦防毒要更新

8.應用系統要更新

9.使用網路要提防

10.電子郵件要過濾

Join at **www.kahoot.it**
or with the **Kahoot! app**

Game PIN:

3372994


感謝聆聽