出國報告（出國類別：其他國際會議）

出席「國際資訊安全會議(DEF CON 24)」報告

服務機關：行政院資通安全處
姓名職稱：周智禾 分析師
派赴國家：美國(拉斯維加斯)
出國期間：105 年 8 月 3 日至 105 年 8 月 9 日
報告日期：105 年 11 月 7 日

摘　　要

近年來網路攻擊事件頻傳，資通安全問題已成為國際關注之重要議題，各國亦定期召開資安相關會議以促進最新資安發展趨勢之交流與分享，包含 RSA Conference、Blackhat 及 DEF CON 等。其中 DEF CON 係全球最知名的駭客技術會議之一，每年定期於美國拉斯維加斯舉辦，內容包含豐富的資安趨勢論壇、最新資安軟硬體設備展覽及國際間最重要的奪旗賽(Capture the Flag, CTF)。

本(105)年(第 24 次)DEF CON 於拉斯維加斯 Paris 和 Bally’s 會議中心舉辦，為期 4 日(8 月 4 至 7 日)，會議內容包括各項軟體的最新漏洞發表，以及時下最熱門的物聯網(Internet of Thing, IoT)安全議題；另本年 CTF 比賽加入一隊機器人菁英隊伍，人類大戰機器人成為本年 DEF CON 注目焦點，而代表我國參賽的隊伍(HITCON)則自 103 年起連續 3 年入選最後決賽，本年最後獲得第 4 名的佳績。

經參加本次會議，建議後續可定期派員參與類此駭客盛會，以掌握最新資安威脅趨勢；建立資通安全科技研發整體規劃與推動機制，以提升國家整體資安自主技術能量；由政府機關主動與相關資安社群合作，進一步帶動資安人才培育，循序充實各層級資安人才。

目　　錄

壹、會議介紹

一、會議名稱

DEF CON 24

二、會議時間

105 年 8 月 4 至 105 年 8 月 7 日

三、會議地點

美國拉斯維加斯 Paris 和 Bally’s 會議中心

四、會議相關文件

會議相關資料請詳見網站(https://www.defcon.org/html/defcon-24/dc-24-index.html)

貳、參加會議目的

DEF CON 為國際間最具名氣的駭客技術會議之一，會議中將發表諸多議題，不論是惡意程式分析、滲透測試技術、數位鑑識及新興漏洞手法等，皆為會議議題之一；迄今已舉辦 24 屆，每年吸引超過 1 萬名的專業資安駭客，以及廠商、政府機關、學研界等資安專業人員齊聚於美國拉斯維加斯，旨在交流資安最新趨勢、攻防最新手法及系統最新弱點。

本次出國主要目的希望能從會議各類議題中瞭解最新資安威脅並掌握國際發展趨勢，除了提升本身對資安議題的認知外，亦期望藉由演講中所獲取的新知與技術，瞭解目前駭客最新的技術，增廣資訊安全上見聞，俾提供業務或決策方面上的協助；另藉由參觀不同主題的駭客村(Villages)，例如 car village、IoT village、social engineering village、crypto and privacy village 及 lockpick village 等，以瞭解不同領域的資安發展趨勢；最後，則是體驗備受矚目的奪旗賽(Capture the Flag, CTF)，見證自動化尋找程式漏洞技術應用在網路攻防戰上之重要里程碑。

參、會議過程及重點議題

一、會議議程

DEF CON 24 演講議程自 8 月 4 日(四)至 8 月 7 日(日)，共分為 4 個廳進行演講，包括「Track 1」、「Track 2」、「Track 3」及「DEF CON 101」，議程詳如表 1 至表 4：

表 1：DEF CON 24 會議第 1 日議程(8 月 4 日)

Time	DEF CON 101
10:00	Machine Duping 101: Pwning Deep Learning Systems Clarence Chio
11:00	Maelstrom - Are You Playing with a Full Deck?... Shane Steiger
12:00	Beyond the MCSE: Red Teaming Active Directory Sean Metcalf
13:00	Weaponize Your Feature Codes Nicholas Rosario (MasterChen)
14:00	Realtime bluetooth device detection with Blue Hydra Zero_Chaos & Granolocks
15:00	Hacker Fundamentals and Cutting Through Abstraction LosT
16:00	DEF CON 101 Panel (Until 17:45)

表 2：DEF CON 24 會議第 2 日議程(8 月 5 日)

Time	TRACK 1	TRACK 2	TRACK 3	DEF CON 101
10:00	Feds and 0Days: From Before Heartbleed to After FBI-Apple Jay Healey	DARPA Cyber Grand Challenge Award Ceremony Mike Walker & Dr. Arati Prabhakar	Introduction the Wichcraft Compiler Collection : Towards universal code Theft Jonathan Brossard (endrazine)	BSODomizer HD: A mischievous FPGA and HDMI platform for the (m) asses Joe Grand (Kingpin)&Zoz
11:00	Compelled Decryption	Project CITL	DEF CON Welcome &	Meet the Feds

	- State of the Art in Doctrinal Perversions Ladar Levison	Mudge Zatko &Sarah Zatko	Badge Talk LOsT & The Dark Tangent	Jonathan Mayer & Panel
12:00	Honey Onions: Exposing Snooping Tor HSDir Relays Guevara Noubir & Amirali Sanatinia	BlockFighting with a Hooker - BlockfFghter2! K2	CAN i haz car secret plz? Javier Vazquez Vidal &Ferdinand Noelsche	411: A framework for managing security alerts Kai Zhong
12:30	Frontrunning The Frontrunners Dr. Paul Vixi		Cheap Tools for Hacking Heavy Trucks Six_Volts &Haystack	
13:00	Research on the Machines: Help the FTC Protect Privacy & Security Terrell McSweeny & Lorrie Cranor	(Ab)using Smart Cities: the dark age of modern mobility Matteo Beccaro & Matteo Collura	How to Make Your Own DEF CON Black Badge Badge Hacker Panel	Sentient Storage - Do SSDs Have a Mind of Their Own? Tom Kopchak
14:00	How to design distributed systems resilient despite malicious participants Radia Perlman	A Monitor Darkly: Reversing and Exploiting Ubiquitous... Ang Cui	Direct Memory Attack the Kernel Ulf Frisk	Anti-Forensics AF int0x80
15:00	How To Remote Control An Airliner: Security Flaws in Avionics Sebastian Westerhold	Slouching Towards Utopia: The State of the Internet Dream Jennifer S. Granick	The Remote Metamorphic Engine: Detecting, Evading, Attacking the AI and Reverse Engineering Amro Abdelgawad	101 Ways to Brick your Hardware Joe FitzPatrick & Joe Grand
16:00	Robot Hacks Video Games: How TASBot Exploits Consoles with Custom Controllers	Side-channel attacks on high-security electronic safe locks Plore	Breaking the Internet of Vibrating Things... follower & goldfisk	
16:30	Allan Cecil (dwangoAC)	Samsung Pay: Tokenized Numbers, Flaws and Issues Salvador Mendoza	Mr. Robot Panel	

17:00	Hacking Next-Gen ATM's From Capture to Cashout. Weston Hecker	Sk3wlDbg: Emulating all (well many) of the things with Ida Chris Eagle		Malware Command and Control Channels: A journey into darkness Brad Woodberg

表 3：DEF CON 24 會議第 3 日議程(8 月 6 日)

Time	TRACK 1	TRACK 2	TRACK 3	DEF CON 101
10:00	How to overthrow a Government Chris Rock	I Fight For The Users, Episode I - Attacks Against Top Consumer Products Zack Fasel & Erin Jacobs	Developing Managed Code Rootkits for the Java Runtime Environment Benjamin Holland (daedared)	Escaping The Sandbox By Not Breaking It Marco Grassi & Qidan He
11:00	Jittery MacGyver: Lessons Learned from Building a Bionic Hand out of a Coffee Maker Evan Booth (Fort)	Light-Weight Protocol! Serious Equipment! Critical Implications! Lucas Lundgren & Neal Hindocha	Picking Bluetooth Low Energy Locks from a Quarter Mile Away Anthony Rose & Ben Ramsey	Secure Penetration Testing Operations: Demonstrated Weaknesses in Learning Material and Tools Wesley McGrew
12:00	Bypassing Captive Portals and Limited Networks Grant Bugher	Stargate: Pivoting Through VNC To Own Internal Networks Yonathan Klijnsma & Dan Tentler	CANSPY: A Framework for Auditing CAN Devices Jonathan-Christofer Demay & Arnaud Lebrun	Attacking Network Infrastructure to Generate a 4 Tb/s DDoS for $5 Luke Young
12:30	Retweet to win: How 50 lines of Python made me the luckiest guy on Twitter Hunter Scott	pin2pwn: How to Root an Embedded Linux Box with a Sewing Needle Brad Dixon		
13:00	Six Degrees of Domain Admin ... Andy Robbins, Rohan Vazarkar, Will Schroeder	MouseJack: Injecting Keystrokes into Wireless Mice Marc Newlin	Cunning with CNG: Soliciting Secrets from Schannel Jake Kambic	NG9-1-1: The Next Generation of Emergency PhOnage CINCVo1FLT & AK3R303
14:00	Weaponizing Data Science for Social Engineering: Automated E2E spear phishing on Twitter Delta Zero & KingPhish3r	Universal Serial aBUSe: Remote physical access attacks Rogan Dawes & Dominic White	Hacker-Machine Interface - State of the Union for SCADA HMI Vulnerabilities Brian Gorenc & Fritz Sands	SITCH - Inexpensive, Coordinated GSM Anomaly Detection ashmastaflash

15:00	Forcing a Targeted LTE Cellphone into Unsafe Network Haoqi Shan & Wanqiao Zhang	Playing Through the Pain? - The Impact of Secrets and Dark Knowledge Richard Thieme	Exploiting and attacking seismological networks.. remotely Bertin Bervis Bonilla & James Jara	Phishing without Failure and Frustration Jay Beale
16:00	"Cyber" Who Done It?! Attribution Analysis Through Arrest History Jake Kouns	DIY Nukeproofing: a new dig at "datamining" 3AlarmLampScooter	I've got 99 Problems, but LittleSnitch ain't one Patrick Wardle	A Journey Through Exploit Mitigation Techniques in iOS Max Bazaliy
16:30		All Your Solar Panels are belong to Me Fred Bret-Mounet	Ask The EFF Panel	Esoteric Exfiltration Willa Cassandra Riggins(abyssknight)
17:00	Drunk Hacker History: Hacker Stories Powered by C2H6O for Fun & Profit Panel	Abusing Bleeding Edge Web Standards for AppSec Glory Bryant Zadegan & Ryan Lester	Crypto State of the Law Nate Cardozo	Sticky Keys To The Kingdom: Pre-auth RCE Is More Common Than You Think Linuz & Medic
17:30				Propaganda and you (and your devices)... The Bob Ross Fan Club

表 4：DEF CON 24 會議第 4 日議程(8 月 7 日)

Time	TRACK 1	TRACK 2	TRACK 3	DEF CON 101
10:00	How to do it Wrong: Smartphone Antivirus and Security Applications Under Fire Stephan Huber & Siegfried Rasthofer	Hacking Hotel Keys and Point of Sale systems ... Weston Hecker	Examining the Internet's pollution Karyn Benson	How to get good seats in the security theater? Hacking boarding passes for fun & profit. Przemek Jaroszewski
11:00	Hiding Wookiees in HTTP - HTTP smuggling... regilero	Discovering and Triangulating Rogue Cell Towers JusticeBeaver	Use Their Machines Against Them: Loading Code with a Copier Mike	Vulnerabilities 101: How to Launch or Improve Your Vulnerability Research Game Joshua Drake & Steve Christey Coley
12:00	Attacking BaseStations - an Odyssey through a	Let's Get Physical: Network Attacks Against	Game over, man! - Reversing Video Games	So you think you want to be a penetration

	Telco's Network Hendrik Schmidt & Brian Butterly	Physical Security Systems Ricky "HeadlessZeke" Lawshae	to Create an Unbeatable AI Player Dan "AltF4" Petro	tester Anch
13:00	Can You Trust Autonomous Vehicles: Contactless Attacks ... Jianhao Liu,Wenyuan Xu,Chen Yan	Drones Hijacking - multi-dimensional attack vectors & countermeasures Aaron Luo	Backdooring the Frontdoor Jmaxxz	Mouse Jiggler Offense and Defense Dr. Phil
14:00	Help, I've got ANTs!!! Tamas Szakaly	An introduction to Pinworm: man in the middle for your metadata bigezy & saci	VLAN hopping, ARP poisoning & MITM Attacks in Virtualized Environments Ronny Bull, Dr. Jeanna N. Matthews, Ms. Kaitlin A. Trumbull	Toxic Proxies - Bypassing HTTPS & VPNs to pwn your online identity Alex Chapman & Paul Stone
15:00	Stumping the Mobile Chipset Adam Donenfeld	Cyber Grand Shellphish Shellphish Panel	Platform Agnostic Kernel Fuzzing James Loureiro & Georgi Geshev	Auditing 6LoWPAN Networks using Standard Penetration Testing Tools Jonathan-Christofer Demay
16:30	Closing Ceremonies			

二、重點議題

(一)CTF 競賽

本年依慣例舉辦 CTF，讓參賽隊伍彼此之間互相攻擊守護的主機，只要奪取對手守護主機內的旗幟檔案即算得分，本次 CTF 重心聚焦到自動化尋找漏洞上，比賽首次加入一隊機器人(可自動尋找程式漏洞並進行修補，甚至利用該漏洞發起攻擊)菁英隊伍，該隊係來自美國國防部國防高等研究計劃署(DARPA)所主辦的 CGC(Cyber Grand Challenge)奪旗賽(如圖 1)冠軍隊伍(Mayhem)，與各國資安高手進行 DEF CON 24 的 CTF 奪旗比賽，人類大戰機器人成為本年 DEF CON 注目焦點，現場參與情況詳見圖 2。

我們能看到自動化的重要性，人類發展自動化已有許久的時間，而能在 CGC 的比賽

中看見這些漏洞尋找的自動化機器人彼此競賽，令資安研究人員相當為之振奮，而 DEF CON 的奪旗賽也將這些自動化尋找漏洞的機器人冠軍隊納入 CTF 比賽隊伍，形成人類與機器之間的奪旗比賽，在資安領域的歷史上已立下了一個新的里程碑。

圖1： DEF CON 24 - CGC 頒獎會議

資料來源： DEF CON 24 官方 Twitter 網頁

圖2： DEF CON 24 CTF 比賽

本次 CTF 最後由美國隊 PPP 奪冠，另代表我國參賽的隊伍(HITCON)則自 103 年起連續 3 年入選最後決賽，本年最終獲得第 4 名的佳績，而本年備受矚目的機器人隊伍(Mayhem)

則敬陪末座，各隊分數如表 1 所示。

表 1：本年 DEF CON CTF 比賽最終成績

Team	Final Score
PPP	113555
blo0p	98891
DEFKOR	97468
HITCON	93539
KaisHack GoN	91331
LC↯BC	84412
Eat Sleep Pwn Repeat	80859
binja	80812
pasten	78518
Shellphish	78044
9447	77722
Dragon Sector	75320
!SpamAndHex	73993
侍	73368
Mayhem	72047

(二)DEF CON Welcome & Badge Talk

每年 DEF CON 的識別證(Badge)都藏著一段秘密等著參加者來發掘，本年也不例外，在 Badge 的掛帶上寫了數組的密碼，參賽者必需蒐集全部的密碼再套上設計者提供的數學公式，解出一組按鍵順序輸入今年的骷髏頭造型 Badge 上，才能看到 Badge 晶片中破解後的燈光，DEF CON 24 的骷髏頭造型 Badge 詳見圖 3。

圖3： DEF CON 24 骷髏頭造型 Badge

(三)Anti-Forensics AF

本場演講中，資安研究員 int 0x80 提出了數個反鑑識的技巧，例如攻擊者如果要防止記憶體鑑識，則可以在執行程式後將記憶體內的 PE Header 部份全部抹去(使用 RtlZeroMemory)，因為 Header 部份在程式讀進記憶體後是不需要的，但後來介入的分析工具卻是需要去讀取記憶體中 Header 資訊來分析接下來的區塊，因此若 Header 資訊消

失則會導致分析工具無法運作。

(四)How to get good seats in the security theater? Hacking boarding passes for fun & profit.

另一個比較有趣的演講係 CERT Polska 的資安研究員 Przemek Jaroszewski 對現在的航班掃描器進行完整的研究，由於現場的登機證都有固定的 Encoding 方式，如紙本的就是 PDF417，手機的就是 QR Code、Aztec 或 DataMatrix，所以研究上要進行解碼並不困難，也有各式各樣的解碼應用程式可供研究，目前登機證常見通用的編碼詳見圖 4。

圖4： 登機證常見通用的編碼

這些常見編碼，被解碼軟體解開之後通常就會是明文方式呈現資料，如班機資訊、登機人姓名、發證時間等等，這種資訊如果被有心人士解開，則可能會帶來個資外洩的風險，登機證編碼解出的明文資訊詳見圖 5。

```
M1JAROSZEWSKI/PRZEMYSLE56XXXX
WAWCPHSK 2762 666M009C0007 666>10B0
K6161BSK 2511799999153830 SK A3
199999999       *3000500A3G
```

Name

圖5： 經解碼過後的登機證資訊

因此接下來，資安研究員 Przemek Jaroszewski 便開始去解讀這些資訊試著竄改資料，然而，這些資訊其實是 Computer Reservation System(CRS)所使用的資訊，而一般航空公司都會使用這套系統，包括一般機場內的休息室也是一樣，並且相關資訊都能在網路上查到文件，因此，講者寫了一個產生器，只要輸入 CRS 系統所需的相關資訊就可以產生 QR Code，CRS 系統 QR Code 產生器功能詳見圖 6。

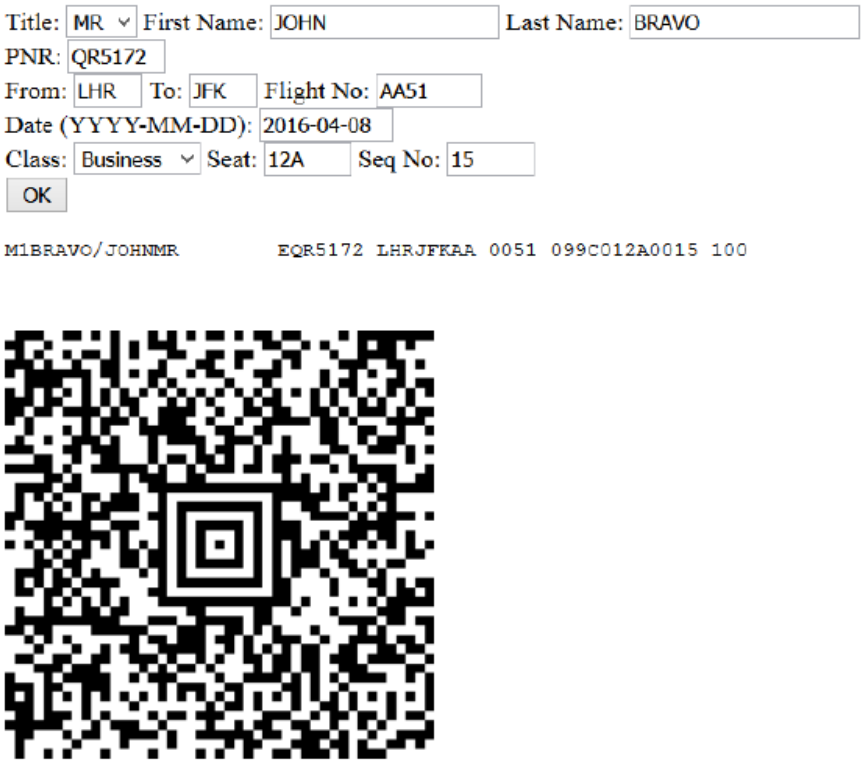


圖6： CRS 系統 QR Code 產生器

利用產生出來的 QR Code，講者可以順利的進入機場休息室，也可以騙過登機證檢查機，當然，紙本類型的 PDF417 也是可以被偽造出來的。

(五)Malware Command and Control Channels: A journey into darkness

在惡意程式分析方面，也有資安研究人員提出新的發現，例如來自 Proofpoint 的資安研究員 Brad Woodberg 就對其公司近期發現的處理事故中，提出了一系列的報告，目前常見的攻擊方法就是駭客寄送社交工程信件，信件上面夾帶著惡意連結，而連結網站則是有 Angler Exploit Kit 所製作，此服務製作出來的網站能自動辨識瀏覽網站的相關資訊，並回傳專門製作的攻擊程式碼，社交工程信件搭配 Angler EK 進行攻擊示意圖詳見圖 7。

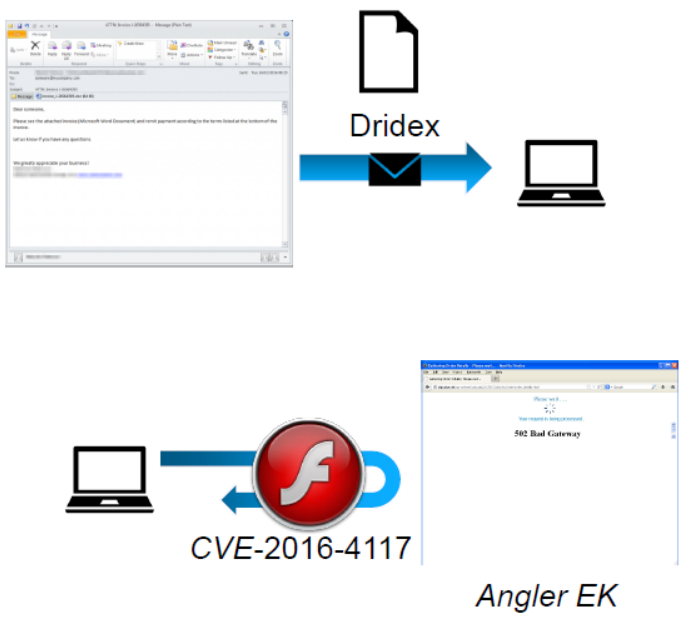
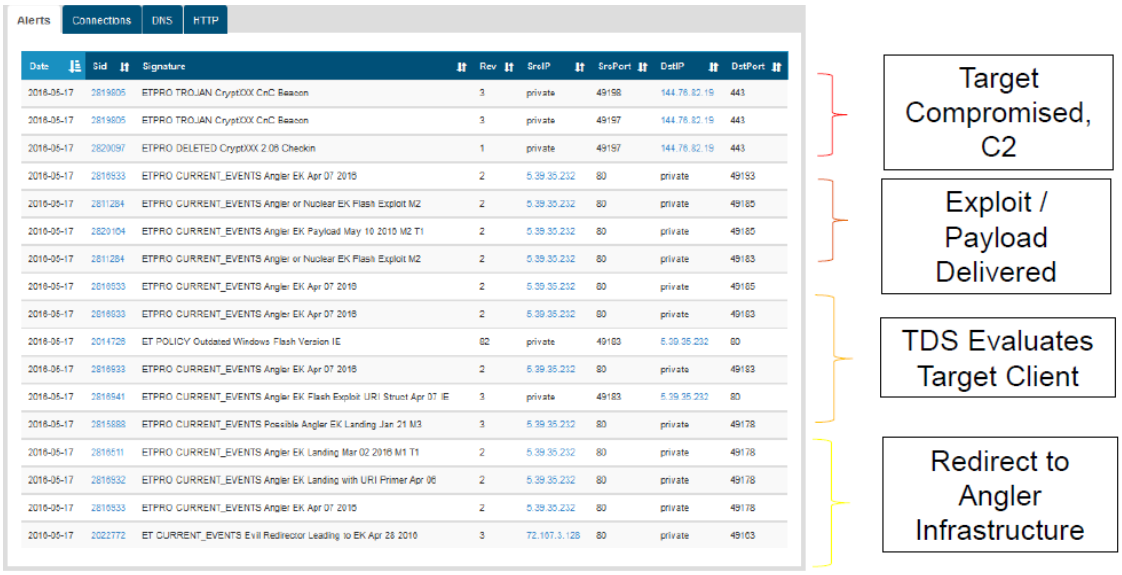


圖7： 社交工程信件搭配 Angler EK 進行攻擊示意圖

若受害端有執行流量監控的話是可以看見這個流程的動作，例如駭客使用 Angler EK 散布 CryptXXX 惡意綁架軟體，則可以看到受害者連到 Angler EK 製作的網站，攻擊成功後受害者連回 Angler EK 報告並下載綁架軟體等的動作，一連串監控網路動作詳見圖 8。



Date	Sid	Signature	Rev	SrcIP	SrcPort	DstIP	DstPort
2016-05-17	2819805	ETPRO TROJAN CryptXXX CnC Beacon	3	private	49158	144.76.82.19	443
2016-05-17	2819805	ETPRO TROJAN CryptXXX CnC Beacon	3	private	49157	144.76.82.19	443
2016-05-17	2820097	ETPRO DELETED CryptXXX 2.06 Checkin	1	private	49157	144.76.82.19	443
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49193
2016-05-17	2811284	ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2	2	5.39.35.232	80	private	49185
2016-05-17	2820104	ETPRO CURRENT_EVENTS Angler EK Payload May 10 2016 M2 T1	2	5.39.35.232	80	private	49185
2016-05-17	2811284	ETPRO CURRENT_EVENTS Angler or Nuclear EK Flash Exploit M2	2	5.39.35.232	80	private	49183
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49185
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49183
2016-05-17	2014726	ET POLICY Outdated Windows Flash Version IE	62	private	49183	5.39.35.232	80
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49183
2016-05-17	2816541	ETPRO CURRENT_EVENTS Angler EK Flash Exploit URI Struct Apr 07 IE	3	private	49183	5.39.35.232	80
2016-05-17	2815888	ETPRO CURRENT_EVENTS Possible Angler EK Landing Jan 21 M3	3	5.39.35.232	80	private	49178
2016-05-17	2816511	ETPRO CURRENT_EVENTS Angler EK Landing Mar 02 2016 M1 T1	2	5.39.35.232	80	private	49178
2016-05-17	2816932	ETPRO CURRENT_EVENTS Angler EK Landing with URI Primer Apr 06	2	5.39.35.232	80	private	49178
2016-05-17	2816933	ETPRO CURRENT_EVENTS Angler EK Apr 07 2016	2	5.39.35.232	80	private	49178
2016-05-17	2022772	ET CURRENT_EVENTS Evil Redirector Leading to EK Apr 28 2016	3	72.167.3.128	80	private	49163

圖8： 流量監控下發現 Angler EK 及綁架軟體的動作

如以防禦的角度而言，許多攻擊都是要投入經費及人力才能達到一定的效果，包括建置監控設備，培養分析人員及資安人才，做為資安廠商的資安研究人員，Brad Woodberg 僅提供參展者相關的資安事故處理經驗，而有無投入資源強化資安方面能量之必要，就需由各資安人共同努力提倡組織內的資安意識。

肆、心得建議

目前國內政府機關所遭受的資安攻擊往往都是駭客精心設計，特別觀察過各個機關網路架構及使用軟體而客制化的攻擊模式，可能是最新的資安漏洞，抑或是尚未發表的零時差(zero day)攻擊，這些攻擊都迫使政府機關必須要做出更嚴密的防禦。每年的DEF CON都是全球資安研究人員的矚目焦點，攻擊國內政府機關的駭客當然也會密切注意，為掌握當前最新威脅趨勢，建議可定期派員參與類此駭客盛會。

此外，國內資安研究多數以網站(Web)安全為重點，抑或進一步瞭解作業系統核心(OS kernel)方面技巧，惟始終脫離不了一般常見的OS框架。目前國內現況可能僅涉及智慧型裝置的資安議題，針對新興議題(如IoT及SCADA)的研究仍顯薄弱，致使資安技術發展不如預期，建議應整合產、政、學、研各界資源，針對不同資安議題投注適合人力及資源並長期關注，以前瞻科技及永續發展為目標，建立資通安全科技研發整體規劃與推動機制，提升國家整體資安自主技術能量，以滿足國內資安防護與維運等工作所需之先進資安技術。

最後，近年我國駭客社群於國際資安競賽屢獲佳績，代表我國的 HITCON 已連續 3 年進入 DEF CON 的 CTF 決賽， HITCON 團隊實力雖持續增加，惟其他國家的代表隊實力亦不容小覷，本年最終 HITCON 獲得第 4 名的佳績，我們也發現目前國內存在頂尖資安菁英量能不足等問題，雖已由行政院國家資通安全會報責成「認知教育及人才培育組」之主辦機關教育部會同科技部、經濟部等共同強化我國資安人才培育事宜，建議後續政府機關可主動與相關資安社群合作，借重其技術能量協助政府機關相關資安檢測、網路攻防及事件處理等，進一步帶動資安人才培育，循序充實各層級資安人才。

伍、會議照片

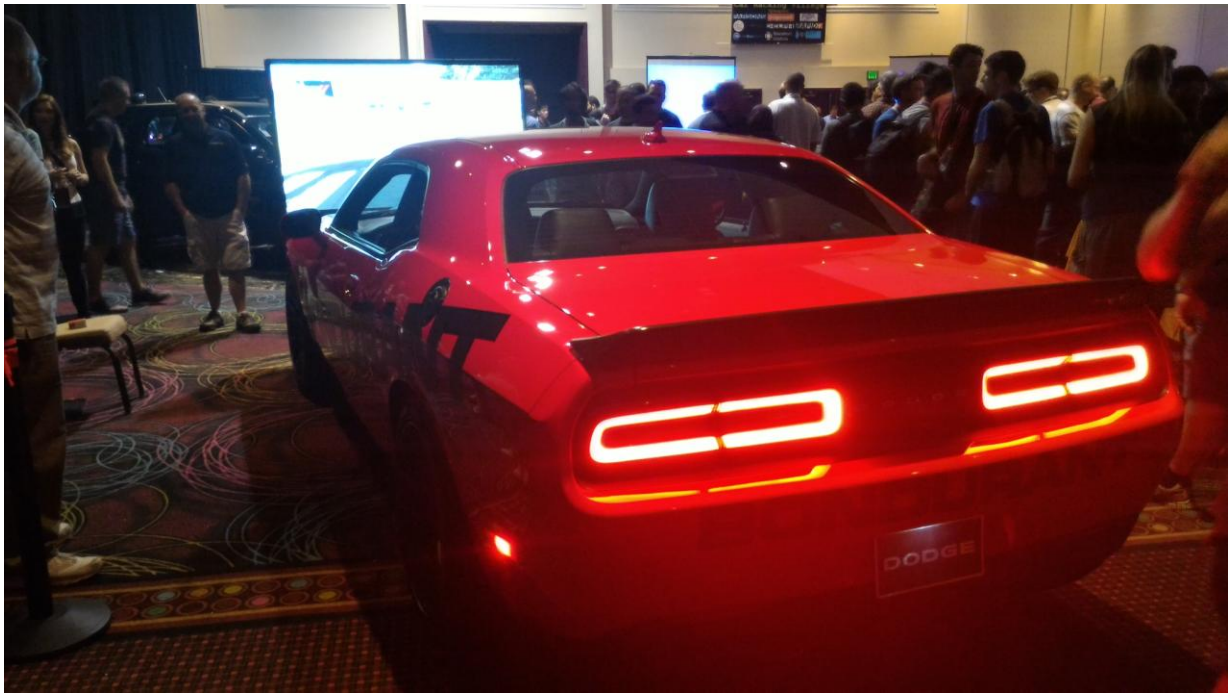


圖 9： Car Village(現場展示賽車模擬遊戲，特別之處在於現場直接放置一部真實的汽車[道奇]，使用者坐在駕駛座操控汽車進行賽車模擬遊戲，汽車則隨著遊戲場景而晃動)

圖 11：CGC 比賽頒獎現場(冠軍為 MAYHEM)

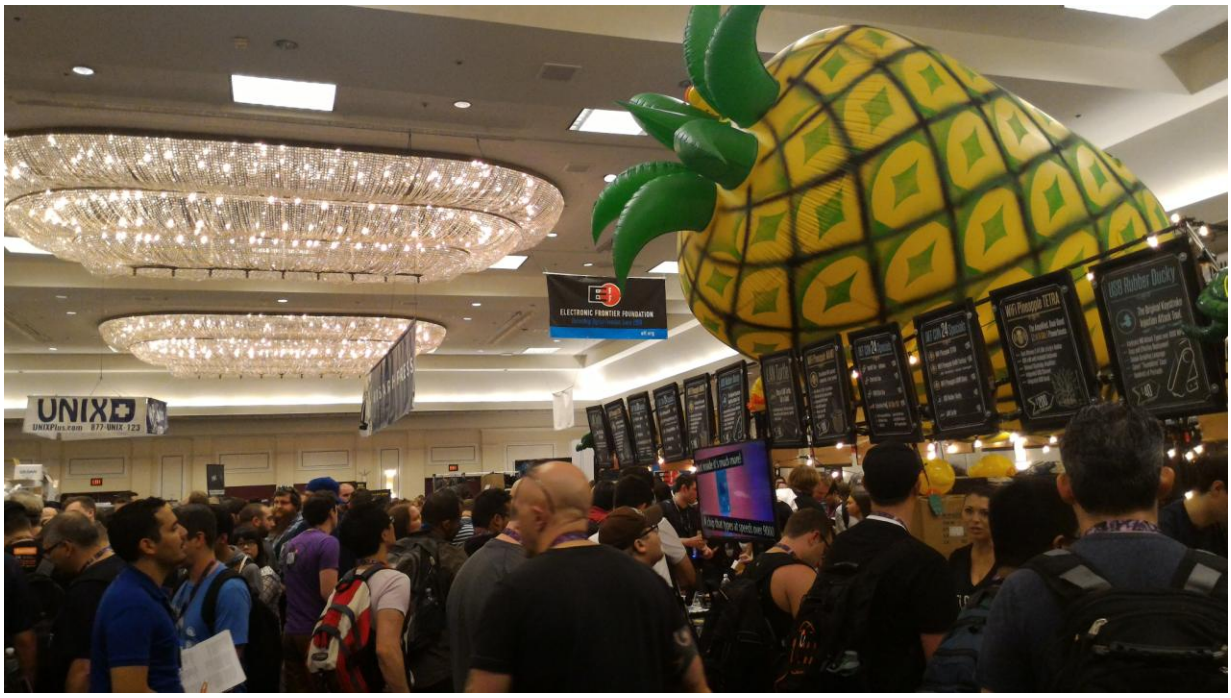


圖 12：廠商展示區(右邊為著名廠商 Pineapple，販賣各種不同的駭客工具，包括無線滲透測試工具、Keystroke Injection 工具等)

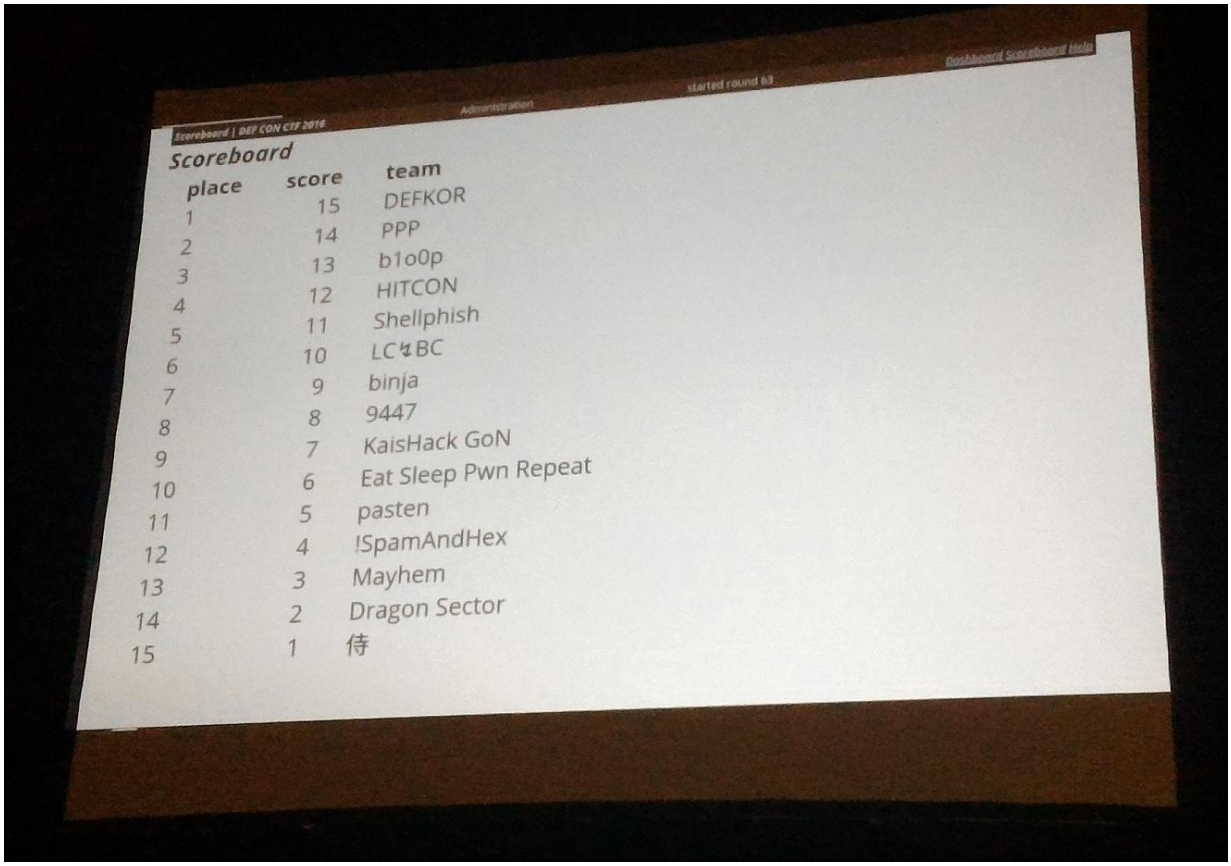


圖 13：CTF 比賽現況排行榜(第 1 天比賽我國代表隊 HITCON 暫列第 4 名)

圖 14：綿羊牆(Wall of Sheep，針對使用會場無線網路但沒做好加密、沒有連上 HTTPS 網站的綿羊網路使用者，將其被監聽到的帳號密碼以部分馬賽克方式，投射在這面牆上)