出國報告（出國類別：視察）

國家通訊傳播委員會參與108年度外交部北美駐外館處資安健診出國報告

服務機關：國家通訊傳播委員會
姓名職稱：周金賢技正
派赴國家/地區：美國洛杉磯、芝加哥及加拿大渥太華、多倫多
出國期間：108年8月5日至108年8月18日
報告日期：108年11月4日

摘要

本專案北美駐外館處資安健診作業 於 2019 年 08 月 05 日至 2019 年 08 月 18 日 於美國洛杉磯、美國芝加哥、加拿大渥太華及加拿大多倫多四個館處進行，此行主要目的透過與國內其他資安團隊合作，協助外交部的駐外館處資安網路進行健診作業，了解目前各外館處資訊設備是否遭受駭客入侵，並檢視其館處是否存在異常無線訊號及網路架構的合理性，以強化外交部的外館單位資安防禦。本次行程依序前往洛杉磯、芝加哥、渥太華及多倫多四個館處進行資訊設備的資安健診，並透過專用檢測工具及團隊合作將發現到的惡意活動進行分析追蹤，協助外館單位找出資安問題並且提供改善建議，並且對外館人員進行資安教育宣導，強化人員的資安防護概念，提升政府單位對於資安防護的重視。

目次

壹、前言.....2
貳、目的、任務編組及健診項目.....2
一、目的.....2
二、任務編組.....2
三、健診項目.....2
參、執行過程.....2
肆、心得與建議事項.....7
一、心得.....7
二、建議事項.....8

國家通訊傳播委員會參與108年度外交部北美駐外館處資安健診報告

壹、前言

本專案北美駐外館處資安健診作業於2019年08月05日至2019年08月18日於美國洛杉磯、美國芝加哥、加拿大渥太華及加拿大多倫多四個館處進行，此行主要目的透過與國內其他資安團隊合作，協助外交部的駐外館處資安網路進行健診作業，了解目前各外館處資訊設備是否遭受駭客入侵，並檢視其館處是否存在異常無線訊號及網路架構的合理性，以強化外交部的外館單位資安防禦。本次行程依序前往洛杉磯、芝加哥、渥太華及多倫多四個代表處（辦事處）進行資訊設備的資安健診，並透過專用檢測工具及團隊合作將發現到的惡意活動進行分析追蹤，協助外館單位找出資安問題並且提供改善建議，並且對外館人員進行資安教育宣導，強化人員的資安防護概念，提升政府單位對於資安防護的重視。

貳、目的、任務編組及健診項目

一、目的

藉由組成網路資安專業團隊，赴駐外館處實地勘察資安防護現況，本專案係協助外交部進行洛杉磯、芝加哥、渥太華及多倫多108年度駐外館處資安健檢，並提供館處改善建議，提升館處資安防護，以降低與外交、國防有關機密情資，藉由駐外館處外洩之可能。本次組團執行資安健診工作的發現事項依規定應屬外交部機密故報告內容主要以作業流程面進行描述。

二、任務編組

健診團隊由外交部、國防部、國家通訊傳播委員會、國安局、行政院國家資通安全會報技術服務中心及財團法人電信技術中心派員編成。

三、健診項目

本次健診團辦理之健診項目包含如下：

（一）資訊資產清點：由外交部代表督導本次健診4個駐外館處之資訊管理人員，辦理該館處之資訊資產清點工作，包括資訊設備品項、數量及使用年限等。

（二）上網電腦與實體隔離電腦資安健診：由健診團針對館處內所有上網電腦與實體隔離電腦，逐一使用健診團準備之健診設備進行資安健診，以清查是否有館處電腦遭受駭客入侵、植入後門程式或感染電腦病毒。

（三）網路環境資安健診：由健診團於滯留館處期間，配合外交部資訊及電務處資安防護及資訊中心，監控、清查館處之電腦網路環境、連外之網路印表機或影印機，並分析館處對外之可疑網路通訊，以釐清有無駭客入侵、列印、影印或掃瞄資料外傳跡象，另由本會與財團法人電信技術中心團員針對館處的無線網路及電信網路架構進行檢測。

參、執行過程

一、行前作業

（一）召開行前會議

健診團隊召開行前會議，向全體團員說明外館資安概況，其次為健診重點單位團員工作分配內容。

（二）健診團隊依工作分配內容準備健診工具與健診項目。

二、健診作業

健診團隊於108年8月5日至8月18日（合計14日）期間，於到達美國洛杉磯辦事處、芝加哥辦事處及加拿大渥太華代表處、多倫多辦事處後，即依任務編組針對健診項目配合執行，除協助館處資訊人員清點資訊資產、全面普查館處所有上網電腦及實體隔離電腦外，並執行電腦資安健診工具派送及電腦運作實況稽核，查察可疑電腦主機及網路通訊，蒐集、分析取得之惡意程式樣本，以追蹤、評估駭客入侵來源與館處受駭範圍，同時協助館處資訊人員隔離受駭設備、辦理系統復原作業，健診作業流程如下：

（一）健診啟始會議

健診團隊到達外館後，先與館處共同召開健診啟始會議，向館處全體人員說明健診團隊來意、介紹成員與健診作業內容。

（二）健診工具設定與執行健診

健診團隊開始執行健診前，為避免健診工具設定失敗，會先確認健診工具與健診資訊蒐集、分析設備間之訊息傳遞正常後，團員再開始執行健診，以降低對館處人員工作之干擾。團員執行健診時由外館聯絡人、資安承辦人員帶領進入館處各單位。

在資安健診過程中團員特別針對事前的情資深入調查，確認是否存在誤判的可能，若發現確實存有高度風險程式或惡意行為，則將深入調查。

三、分析結果相關作業

（一）分析駭侵情資及研擬建議作為

健診作業實施後，若發現有主機存在駭侵情資，健診團隊整合團隊力量共同分析情資，以儘速於健診作業期間瞭解駭侵行為態樣，提供外交部參用。

（二）製作健診結果會議簡報

健診結果會議簡報於會議前一日製作完成，依北美健診結果會議之模式，大綱分為：依據及目的、健診結果、中毒電腦分析、高風險程式、其他所見情形及建議事項等章節。

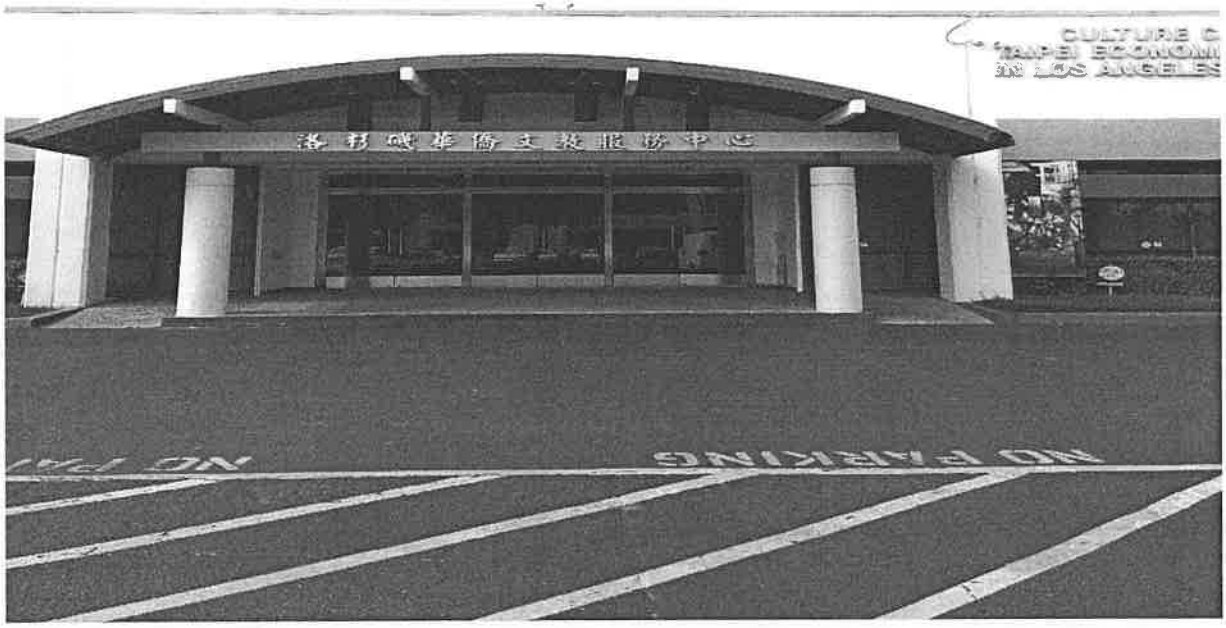
四、健診結案會議

健診結案會議以簡報方式向館處相關人員說明健診結果及改善建議，並協助回應館處人員資安問題，如屬決策性管理問題，則交由外交部統一回應。在結案會議前團員會將發現的缺失部分立即協助改善，若無法現場改善的部分則會交由館處的資安官協助後續處理。

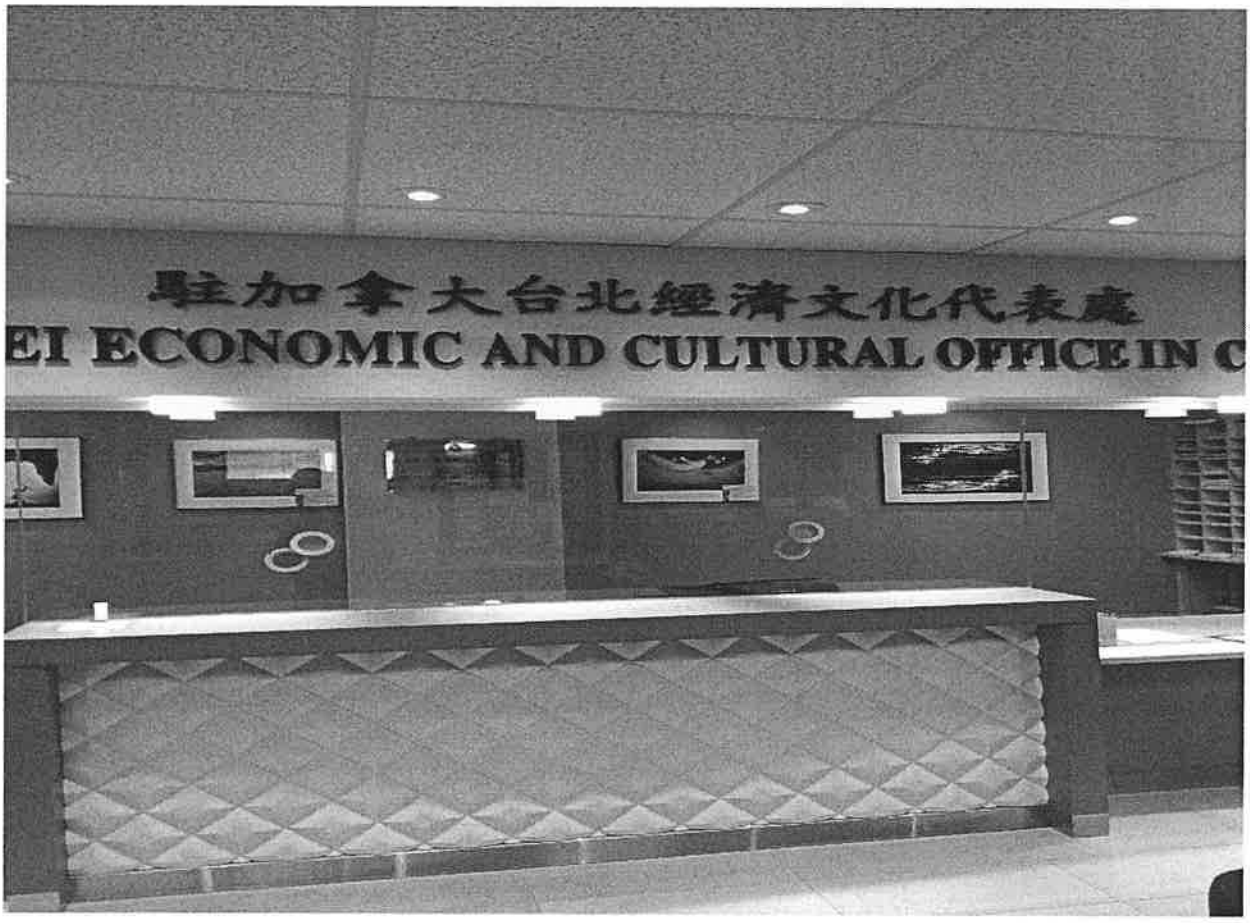
資安健診行程表

日期	工作地點	工作內容
8月5日	桃園機場 → 美國洛杉磯辦事處	1、出發行程。 2、至美國洛杉磯辦事處檢整健診工具及向團員進行任務提示。
8月6日～8月8日	美國洛杉磯辦事處	1、執行館處電腦資安健診作業及每日成果報告。 2、美國洛杉磯辦事處資安健診總結報告。
8月9日	美國洛杉磯辦事處 → 芝加哥辦事處	至芝加哥辦事處檢整健診工具。
8月10日～8月11日	芝加哥辦事處	執行館處電腦資安健診作業及每日成果報告。
8月12日	芝加哥辦事處 → 加拿大渥太華代表處	1、芝加哥辦事處資安健診總結報告。 2、至加拿大渥太華代表處檢整健診工具。
8月13日～8月14日	加拿大渥太華代表處	執行館處電腦資安健診作業及每日成果報告。
8月15日	加拿大渥太華代表處 →多倫多辦事處	1、加拿大渥太華代表處資安健診總結報告。 2、至多倫多辦事處檢整健診工具。
8月16日	多倫多辦事處	1、執行館處電腦資安健診作業及每日成果報告。 2、多倫多辦事處資安健診總結報告。
8月17日	多倫多辦事處 →桃園機場	2、回國行程。

工作概況照片




處事辦化文濟經北台哥加芝駐
TAIPEI ECONOMIC AND CULTURAL OFFICE IN CHICAGO


駐加拿大台北經濟文化代表處
EI ECONOMIC AND CULTURAL OFFICE IN C

肆、心得與建議事項

一、心得

本次奉派參與資安健診團隊，為從事公職生涯首次參與防制駭客之資安技術實務工作，隨著團隊成員一同檢視健診工具分析結果，並由蒐集之駭客入侵跡證中，逐漸抽絲剝繭，瞭解駭客入侵之路徑與手法，整個過程實是一大挑戰。由於駐外館處本身亦有資訊管理相關人員配合進行定常資安防護工作，是以團隊每到 1 個館處，要從蒐集跡證瞭解駭客如何入侵之詳細過程，加以駭客有意掩藏行跡，查察過程並不容易，實務上涉及多項電腦、網路資訊技術，需要團隊成員共同貢獻自身專業知識及經驗，並透過討論方能確認。惟此類資安專業技術，一方面需要具有多種電腦程式語言基礎，以研判駭客所使用之程式語言，看懂駭侵程式及其來源去向，俾利追根究底取得更進一步之駭侵資訊；另一方面亦需多方涉獵電腦操作系統底層資訊，瞭解電腦操作系統架構，並長期累積駭客常用手法資訊，方能在短暫期間內，快速由取得跡證研判出駭侵手法。

本次專案執行過程中，依照團隊分工作業流程，特由電信技術中心及本會團員針對館處的無線網路及電信網路架構進行檢測，大大改善外館無線網路訊號品質，並強化了外交部的外館資安防禦能力，認為本會隨團所負責之項目是對他們有幫助且期待已久的服務。

另由駭侵行為發現，會經常攻擊不熟悉電腦之初學者及第 1 線受理陳情人員，而機關資訊部門亦不能僅倚靠單一防毒軟體從事全機關防毒，即可認為天下太平。在加密技術的強力支援下，資安部門與駭客的攻防拉鋸戰將持續發酵中。

二、建議事項

本次資安健診團隊對於館處資安防護之建議事項如下：

1、嚴禁使用上網電腦儲存或處理公務資料，勿將私人設備連接公務電腦使用。

2、針對此次健診發現之樣本特徵行為納入單位防火牆、防毒軟體及健診掃瞄工具，以強化資安設備防護能力。

3、關閉非必要網路服務埠，並定時更新作業系統漏洞修補。

4、掃毒電腦為館處人員隨身碟，及執行資料交換重要平臺，應隨時更新病毒碼，避免遭惡意程式感染。

5、定時將上網電腦及實體隔離電腦防毒軟體病毒碼更新。

6、確實設定密碼，並符合複雜度要求。

7、發現異常郵件不隨意點擊，並主動聯繫資安官協查。

8、本次專案執行後，依照本會與電信技術中心團員針對館處的無線網路及電信網路架構之檢測結果執行相關工作。