2017資安年刊

2017資安年刊

前言

網路世界為人們帶來便利，相對而言也帶來了風險，因此資訊安全成了現今社會所關注的重要議題之一，資訊安全若沒有完善，則有可能會產生許多不可預期的損失，像是機關電腦資料遭竊、帳號密碼遭盜用、金融機構遭駭侵盜領、勒索軟體威脅、電腦病毒發作及網頁遭置換等，資訊網路時代雖帶來便利但也同時讓自身暴露於危害之中。眾多的資安威脅不斷影響個人、企業、甚至是國家層級的安全性，為了能夠因應各種網路攻擊事件，因此需要一個能夠統籌、協調的組織，針對這些資安事件進行掌握及協助，因此才有電腦網路危機緊急應變處理團隊(Computer Emergency Response Team, CERT)/電腦安全事件應變團隊(Computer Security Incident Response Team, CSIRT)的產生。

目前我國政府部門、通訊傳播事業、教育部、國家高速網路與計算中心、電子交易平台、資訊產品服務等公私部門，皆已建構各自CERT/CSIRT，上述緊急應變組織都具有垂直單線式資安事件通報應變作業處理流程，惟仍須建立國家層級之資安事件處理協調中心，採取積極、主動之作為，強化CERT/CSIRT橫向溝通機制，以處理各界所發生之網路威脅事件，且若發生跨國或跨單位之威脅事件，為使各組織間資訊暢通、快速分享所獲情資並協調事件應處單位，應建構各CERT之間密切聯繫管道，透過互信互利之聯盟機制，以了解全台資安態勢樣貌，強化國內各界資安防護能量，協助推動資安相關活動，建構我國安全網路使用環境。

台灣電腦網路危機處理暨協調中心(Taiwan Computer Emergency Response Team/Coordination Center，TWCERT/CC)於民國87年9月由中山大學成立，民國99年1月由台灣網路資訊中心(Taiwan Network Information Center，TWNIC)接手維運，而2014年8月起改由國家中山科學研究院承接，並於2015年4月完成改組(如圖1)，在行政院資通安全辦公室(現為行政院資通安全處)指導下重新運作。為了提升台灣整體資安防護能量，TWCERT/CC主導推動資安事件通報、資安教學資源提供及舉辦資安宣導活動等項工作。經由政府指導，透過與國內外CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業等多元化合作，並進行資源整合，共同維護台灣整體網路安全穩健。從安全、便利、效能三面向來推動資通安全，以建構國家資安聯防體系、推升資安產業自主防護能量、孕育優質資安菁英人才及強化公私協同合作機制，期逐步實現「建構網路安全環境，邁向優質網路社會」之願景。

前言

TWCERT/CC主要目標為建立對民間資安事件支援及服務的能量及跨國網路安全情資共享管道，並提升整體資安聯防與應變能力，平時推動民間資安事件通報及協處、擔任國內外資安事件應處協調窗口、蒐整與分享國內外資安情資、強化民間資安意識及舉辦資安宣導會議等項工作。

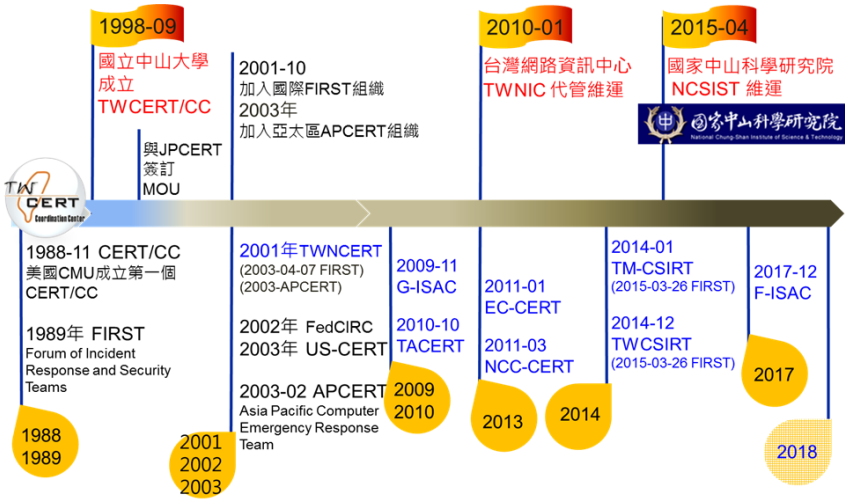

圖1 TWCERT/CC歷史沿革

TWCERT/CC為提升我國整體資安環境，將積極與民間組織建立合作夥伴關係，並鼓勵資安事件通報意願，建立資安聯防體系與能量。且配合各企業組織/產業公協會相關活動辦理座談會、教育訓練等，宣導及輔導民間建立CSIRT，以達到提升民間資安自主防護能量及資安聯防的目的，並透過研討會了解民間組織之想法，進而滾動修訂資安通報作業流程、資安事件通報單、通報內容之安全管控、資料保護宣告等。

TWCERT/CC平時主要提供民間服務有四項：

1.事件通報處理

提供民間企業團體和個人多元通報方式，根據事件緊急程度給予相應的技術諮詢、建議和協助。目前可透過TWCERT/CC E-mail、電話及官網等多項通報管道，提供事件相關人聯絡資訊、受害主機資訊及事件發生描述，即可進行通報。若提供更詳細的系統資訊(Log)，對於事件處理更有幫助。

2.事件應變協調

協助國內民間企業組織/產業公會成立CERT/CSIRT，以建立組織內部事件應變能力，當事件發生時，TWCERT/CC也會以事件影響等級協調國內外資安組織進行事件應處。

前言

3.情資整合發布

與國際資安組織合作交流並分享情資，如反釣魚工作小組(Anti-Phishing Working Group, APWG)、美國國土安全部(DHS)之NCCIC Portal及自動化資安威脅情資共享計畫(Automated Indicator Sharing, AIS)、No More Ransom專案、STOP.THINK.CONNECT與Cyber Security Awareness Month(NCSAM)Champion及Data Privacy Day Champion會員、雲端安聯盟(Cloud Security Alliance, CSA)之情資分享系統(Intelligence Exchange)及APCERT惡意緩解工作小組之Lebahnet誘捕系統計畫等國際資安合作。將取得的情資彙整研析追蹤，掌握國內外重大資安事件發展，推測研判網路威脅態勢，以提供決策單位參考。

4.技術研究發展

持續發展資訊系統，如建立TWCERT-ISAC(Information Sharing and Analysis Center；資安資訊分享與分析中心)，接軌國內外交流平台，服務企業與民眾，以強化國內外情資聯防效益，提升我國資安事件預警與應處能力。並與國家高速網路與計算中心(以下簡稱國網中心)合作開發惡意樣本檢測系統MARS(Malware Analysis & Report System)，提供政府及民間簡捷的惡意樣本上傳介面，經國網中心沙箱分析後，產出報告予使用者，透過直接上傳惡意樣本至MARS系統，以避免機敏資料外洩疑慮。

如何確保所處在的網路環境下是安全的，已成為當今重要議題之一，資通訊科技(ICT)的迅速發展，帶來了便利與智慧化的生活，同時也衍生了資訊安全的疑慮：對個人，造成個資外洩、檔案勒索或財務盜刷；對企業，造成經濟損失、商譽受損或機密外洩；對國家，關鍵資訊基礎設施遭駭，引發政經民心動亂，政府已將資訊安全提升到國家安全的層級，因此，本刊將透過五個章節來陳述及宣導資訊安全的觀念應成為國民的基本素養。第一章節針對資安聯防新思維介紹；第二章節則以TWCERT/CC於2017年資安通報現況及案例進行說明;第三章節闡述TWCERT/CC於2017年主要資安事件及分析建議結果；第四章將介紹目前開發中的情資交換平台TWCERT-ISAC相關功能與服務進行介紹；此外，TWCERT/CC平時也積極與國內外資安組織合作及辦理資安研討會議，將於最後一個章節作介紹。

資安聯防新思維

資安聯防新思維

隨著時代的演進及科技的進步，從小至個人手機、家電，大至國家油水電等關鍵基礎設施，有許多設備漸漸都可連上網路，駭客攻擊的手段也愈趨多樣化，資訊安全已不再只是專業人士的責任，若資安沒有做好，輕則個人可能會造成財產上的損失，重則嚴重影響國家安全，因此政府訂出「資安即國安」的這項政策。目前企業組織及產業公協會所缺乏的就是資安事件應變團隊，若企業中有專屬的資安事件應變團隊，平時不僅可蒐集特定情資分享給內部人員提升資安意識，事件發生時也有相對應的應變機制及團隊可以立即處理，以減低事件影響的損害。此外，若成立CSIRT，平時可針對該產業相關資安事件威脅進行蒐整，以掌握最新趨勢，提早採取相關防範措施，而若發生事件時，也可將事件的狀況及處理的經驗，透過去識別化的方式分享給同業其他夥伴，藉由這種互動方式，達到資安聯防的目的。

世界各國已有成立CSIRT聯盟組織，如日本有成立CSIRT聯盟(Nippon CSIRT Association, NCA)，主要針對民間企業進行CSIRT建置推廣，並定期召開聯盟會議，針對特定的議題進行探討。囿於TWCERT/CC負責協助民間企業組織/產業公協會提升資安自主防護能量，目前也積極廣推民間企業組織/產業公協會建置CSIRT，期望未來也可仿照日本建置CSIRT聯盟，制定民間組織資安聯防機制。然而台灣目前其實有許多CERT/CSIRT分別於各公私部門中運作，但皆無共同定期聚會，期望建立定期性的CERT/CSIRT會議，讓各CERT/CSIRT保持聯繫，透過互信互利之聯盟運作，以了解全台資安態勢樣貌，強化國內各界資安防護能量，互通國內資安情資交流，協助政府推動資安政策與活動，建構我國安全網路使用環境。因此，TWCERT/CC於2016年10月開始主動召集各CERT/CSIRT組成「台灣CERT/CSIRT聯盟」，透過定期召開會議，交換意見並密切合作，了解目前資安態勢，以達資安聯防目的，共同維護台灣網路安全之穩健性。

資安事件處理過程可以分為事前、事中、事後，事前使用SOC(Security Operation Center)進行網路流量監控，以確保無異常狀態；而當事件發生時則會有CERT/CSIRT事件應變團隊進行通報及處置；事後則針對該事件的狀態透過ISAC(Information Sharing and Analysis Center)進行分享，透過情資互享的方式讓大家了解事件的狀況，針對潛在威脅進行預警防護，今日資安態勢已不再是單打獨鬥的方式，透過情資交換，才能達到情資整合聯防的最終目的，接續將特別針對CSIRT及ISAC進行介紹。

一、台灣CERT/CSIRT聯盟

TWCERT/CC為扮演國際與國內資安事件處理的協調角色，與國內外資安組織緊密聯繫與合作，加速事件協調與處理時效，提升整體資安聯防與應變能力。另外，我國目前在多個公私部門中，已建立各自之電腦網路危機處理小組，例如政府部門、通訊傳播事業、學術界、學術研究單位、電商業者、資安公司和會計事務所(如下表)，為建立各CERT間橫向聯繫之溝通管道，使資安訊息傳遞順暢，並於發生資安事件時協調各單位進行處理作業，TWCERT/CC已於2016年度推動「台灣CERT/CSIRT聯盟」(如圖2)，後續將協助國內尚未成立CERT/CSIRT之領域，提供建立CERT/CSIRT之準則及所需的協助，透過互信互利之聯盟運作，強化國內各領域資安防護能量，互通資安情資分享，配合政府推動資安政策與活動，建構我國安全網路使用環境。

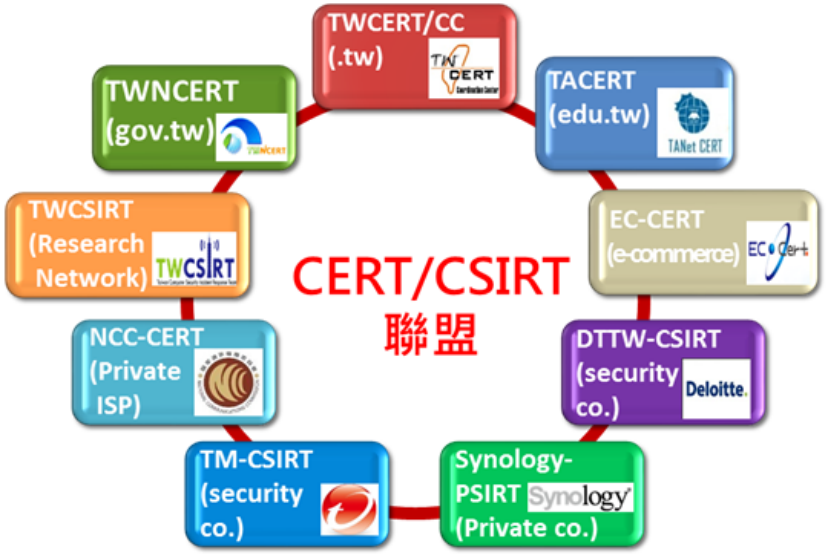

圖2 台灣CERT/CSIRT聯盟

一、台灣CERT/CSIRT聯盟

表1 台灣CERT/CSIRT聯盟

服務範圍	CERT/CSIRT中文名稱	CERT/CSIRT英文名稱
政府部門	國家電腦事件處理中心	TWNCERT(Taiwan National Computer Emergency Response
通訊傳播事業	國家通訊傳播委員會	NCC-CERT(National Communications Commission Computer Emergency Response Team)
學術網路	台灣學術網路危機處理中心	TACERT(Taiwan Academic Network Computer Emergency Response Team)
研究單位	台灣電腦安全事件應變中心	TWCSIRT(Taiwan Computer Security Incident Response
企業內部私人應變團隊	群暉科技 - 產品安全事件應變團隊	Synology-PSIRT(Product Security Incident Response Team)
電商業者	電子商務資安服務中心	EC-CERT(Electronic Commerce – Computer Emergency
資安公司	趨勢科技股份有限公司	TM-CSIRT(Trend Micro Computer Security Incident
會計事務所	勤業眾信	DTTW-CSIRT(Deloitte Taiwan Computer Security Incident
中小企業	台灣電腦網路危機處理暨協調中心	TWCERT/CC(Taiwan Computer Emergency Response Team /

一、台灣CERT/CSIRT聯盟

藉由建立定期性的「台灣CERT/CSIRT聯盟」會議，讓台灣目前各CERT/CSIRT有固定聯繫管道，透過互信互利之聯盟運作，強化國內資安防護能量，互通國內資安情資，協助政府推動資安政策與活動，建構我國安全網路使用環境。2017年已於7月17日及10月27日舉辦2017年度第一次及第二次「台灣CERT/CSIRT聯盟會議」(如圖3、圖4)，會議由TWCERT/CC主辦，第一次及第二次會議有TWNCERT、TWCSIRT、TACERT、TM-CSIRT、EC-CERT及NCC-CERT共同參與，其中第二次會議邀請勤業眾信的CSIRT(DTTW-CSIRT)及群暉科技的PSIRT參加台灣「CERT/CSIRT聯盟」會議，會中各單位進行近期執行狀況及成果分享。透過定期聯盟會議的方式，可了解彼此各CERT/CSIRT執行近況，或於會中針對特定議題進行探討。

圖3 第一次「台灣CERT/CSIRT聯盟會議」

圖4 第二次「台灣CERT/CSIRT聯盟會議」

二、資安通報應變與情資分享機制

(一)資安通報CSIRT介紹

台灣企業組織/產業公會建立電腦安全事件應變小組主要任務乃針對產業或企業內資安事件通報接收與分享、並針對通報事件進行分析應變，以及主導產業與企業內之資安教育和監控等。旨在有效的處理資安事件，建立與強化產業與企業組織資安事件應變機制，提升產業與企業組織內部之資安意識，以降低企業關鍵營運業務風險。

目前我國政府部門、通訊傳播事業、教育部、國家高速網路、電子交易平台、資訊產品服務等，皆已建構各自電腦網路危機緊急應變處理中心，大多數的企業內部都已制定資安事件的處理方式，然而，其中只有少數幾家公司已經建立了企業範圍的資安事件應變架構，而網路安全問題所造成的威脅及層面並非特定產業所有，往往因重大的資安事件而威脅到核心業務營運。因此透過企業/產業現有的基礎，來有效運用資安事件處理資源，是有其必要建立自身之CSIRT。

為健全我國緊急應變組織，本中心研擬「TWCERT/CC企業資通安全事件通報應變作業綱要」及「民間企業組織/產業公會CSIRT 建置實務指引」，提供企業於發現資通訊系統遭受破壞與不當使用等資通安全事件時，能有一回報與協處管道，透過快速通報及緊急應變處理，能在最短時間內讓受駭系統恢復正常，將災損減至最低，以確保企業之利益與正常運作，並協助各企業組織/產業公會培育建置各自之CERT/CSIRT機制。

TWCERT/CC也透過「台灣CERT/CSIRT聯盟」強化橫向成員間資訊的串聯，分享處理資安事件所累積之應處經驗與專業知識，並加以有效適當的分工協同合作，加速事件通報與處理時效，進而形成資安防護連線。

另為強化資安事件的通報處理、應變協調、情資發布和交流合作效益，透過建置TWCERT-ISAC，以整合資安資訊，提升威脅情資預警聯防效益。

二、資安通報應變與情資分享機制

(二)情資分享ISAC介紹

資安資訊分享與分析中心其主要目的為情資之蒐集、分析及交換，透過蒐整資安相關情資及弱點資訊，將其分類並提供分析結果及對策，針對可能之威脅進行預警防護；此外，會員間進行情資交流，強化情資分享與協調聯防機制，透過分享資安相關情資與分析報告，以利決策者與資安防護人員有效因應資安事件。

ISAC的概念是根據1998年美國總統決策指令(Presidential Decision Directive 63, PDD-63)，要求政府機關與民間單位應識別與分享其網際網路或實體相關之威脅、弱點及資安事件，以保護國家重要的基礎建設。綜觀國際之ISAC發展，依美國負責跨領域ISAC管理之組織National Council of ISACs(NCI)，現行已涵蓋24個產業ISAC。

我國於民國90年成立「行政院國家資通安全會報」，負責推動我國資通安全基礎設施工作，自97年起推動跨領域之資安資訊分享與分析工作，而「政府資安資訊分享與分析中心(G-ISAC)」於98年11月正式運作，期結合政府與民間之力量，透過G-ISAC情資格式標準化與系統自動化之情資分享機制，讓會員間彼此整合、分享資安情資，以達成資安預警效益及各領域間橫向之資安聯防目標，此外，鑑於國內外資安情資來源漸趨多元，情資日益增加，因此我國於將於2018年建立國家層級ISAC(National ISAC, N-ISAC)，以提升國家整體資安應變與防護能力。

資安通報現況與案例

資安通報現況與案例

發生資安事件時，CERT/CSIRT會執行通報應變作業，TWCERT/CC通報業務中，其通報情資來源非常廣泛，除了國內企業組織、學研單位、資安機構，以及駭客社群等單位外，也與國際CERT/CSIRT、資安相關單位等進行合作，於2017年度，分別從國內及國外等眾多單位通報而來的情資，從1月至12月共計接收8,721筆資安通報情資，其中通報來源筆數最多的是美國。而在TWCERT/CC接收到情資後，會針對該情資進行研判，若為國內資安事件會透過G-ISAC通報到相關單位進行處理；若為民間企業組織通報特定資安事件，TWCERT/CC會直接處理；而若情資屬於國外資安事件，則會通報到國外相關單位協請處理，例如：「有某單位通報該系統顯示，有惡意IP持續攻打其網路設備，TWCERT/CC經研判後，發現其IP為美國IP，TWCERT/CC將會通報美國US-CERT及所屬ISP業者，請其協助處理。」2017年度1月至12月共有1,847筆協助通報至國外。以下將以TWCERT/CC在2017年度資安通報現況說明，及針對TWCERT/CC協助受事件影響之民間企業單位進行通報處理之重要或特殊案例介紹。

一、2017年資安通報現況

(一)協助國內資安事件通報與處理並分享於政府資安資訊分享與分析中心(G-ISAC)

TWCERT/CC於2017年1月至12月共計接收8,721筆資安通報情資，依國別區分，以台灣來的情資為大宗，其後依序為美國、英國及新加坡(如圖5)。美方提供我方多數資安情資通報，其他國家資安廠商情資分享相對數量較少，TWCERT/CC未來賡續與他國資安組織建立情資互享之聯繫管道，以更能及時取得國際資安情資。

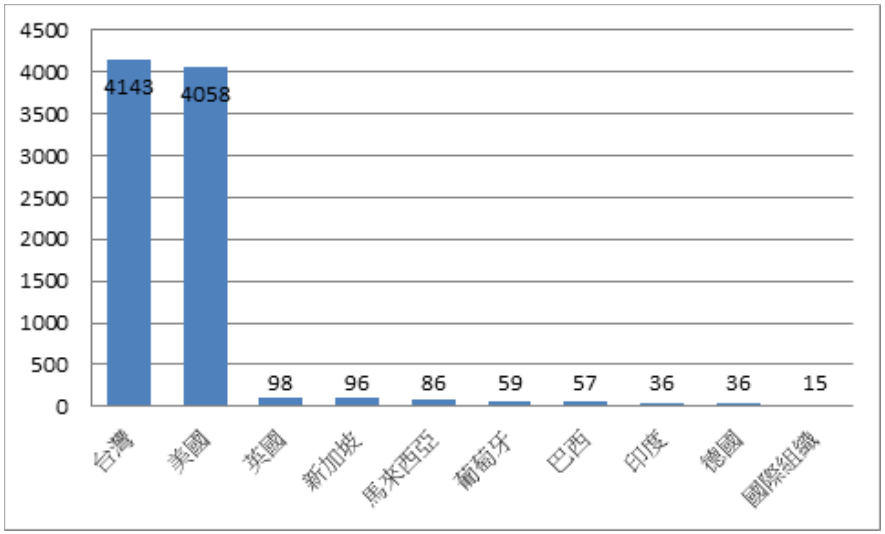

圖5 2017年度TWCERT/CC所接收之資安事件通報數量前10名(以國別統計)

一、2017年資安通報現況

經通報人員確認資安事件為台灣IP，並對情報內容進行了解與分類，類別包括資安情報(ANA)、網頁攻擊情報(DEF)、資安預警情報(EWA)及入侵攻擊情報(INT)等四類(如右表2)，再經由「政府資安資訊分享與分析中心(G-ISAC)」通報分享平台進行情資分享，G-ISAC通報分享平台會將情資資訊通報給相關單位，該等單位依影響等級回饋相關處理作為至G-ISAC通報分享平台，以協助TWCERT/CC進行事件追蹤與控管，國內通報作業流程如圖6。

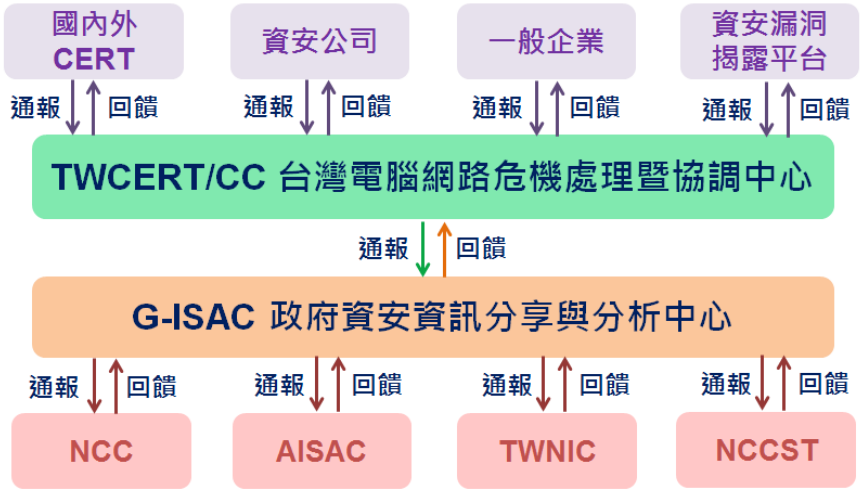

圖6 國內通報作業流程

表2 通報情資分類表 (引用行政院技服中心G-ISAC事件類型定義說明)

分類	通報類型
資安訊息情報(ANA)	漏洞訊息、攻擊活動訊息、服務訊息、中繼站黑名單、惡意程式樣本等。
網頁攻擊情報(DEF)	網頁置換、惡意留言、惡意網頁、網頁木馬、釣魚網頁、個資外洩等。
資安預警情報(EWA)	系統疑存在弱點、可疑連線、資訊疑遭洩漏、存在可疑程式、疑發起對外攻擊、疑發送垃圾郵件(Spam)等。
入侵攻擊情報(INT)	系統被入侵、對外攻擊、散播惡意程式、殭屍電腦(Bot)、電子郵件社交工程攻擊、垃圾郵件(Spam)等。

一、2017年資安通報現況

表3 通報GISAC資安事件筆數統計表

月份	資安訊息ANA	網頁攻擊DEF	入侵攻擊INT	資安預警EWA	小計
2017/1	1	10	48	3	62
2017/2	3	20	47	4	74
2017/3	101	13	54	10	178
2017/4	3	14	27	23	67
2017/5	6	25	167	1	199
2017/6	3	33	371	3	410
2017/7	1	22	1193	11	1227
2017/8	9	25	1030	16	1080
2017/9	5	10	669	45	729
2017/10	2	18	61	35	116
2017/11	15	14	198	54	281
2017/12	4	13	76	204	297
合計	153	217	3941	409	4720

針對2017年度國內資安事件通報應變，TWCERT/CC協助國內資安事件通報與處理流程，通報對象主要為國家通訊傳播委員會(NCC)、教育學術資訊分享與分析中心(AISAC)與台灣網路資訊中心(TWNIC)三個單位。對外則是協調與追蹤國外ISP業者與相關CERT，協助進行國際資安事件之處理。2017年1月至12月通報至G-ISAC計4,720筆，已超過去年(2016年)總筆數(去年通報總數為3,461筆)，其中以入侵攻擊情報(INT)3,865筆最多，除6月開始新增APWG及主動發掘zone-h等情資外，7月起擴展AIS計畫情資的管道，因此通報數高於其他月份，詳細清單參照表3及圖7。

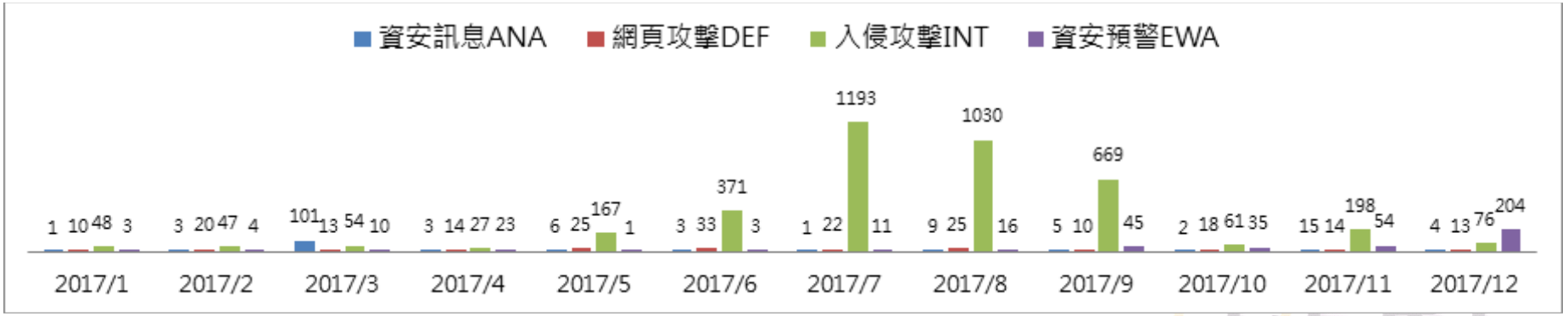

圖7 TWCERT/CC分享資安通報至G-ISAC筆數統計圖

一、2017年資安通報現況

(二)協調國外通報資安事件處理

TWCERT/CC通報應變小組每日經通報人員確認所接收之資安事件為國外IP，並對情報內容進行了解與分類後，再經由Email通報IP所屬之業者或ISP業者及相關CERT單位，通報作業流程如圖8。TWCERT/CC於2017年1月至12月協助通報至國外共1,847筆(如圖9)，透過事件通報到國際CERT/CSIRT，提供事件協助，除善盡國際資通安全維護責任、提升我國際能見度及友好形象，並藉以建立國際聯防機制及強化我資訊安全風險管理之認知與能力。

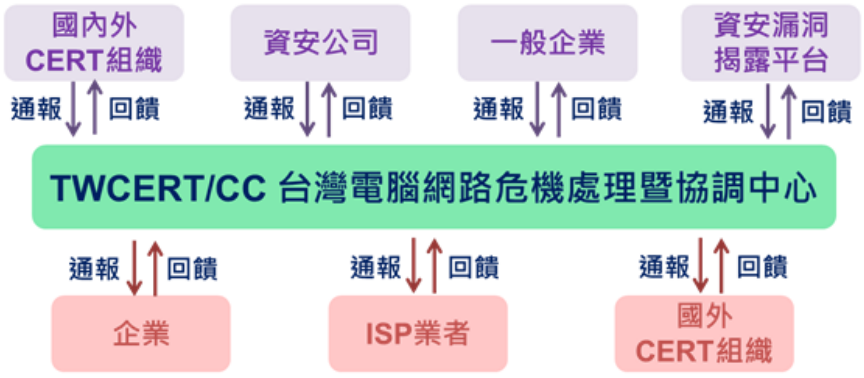

圖8 國外通報作業流程

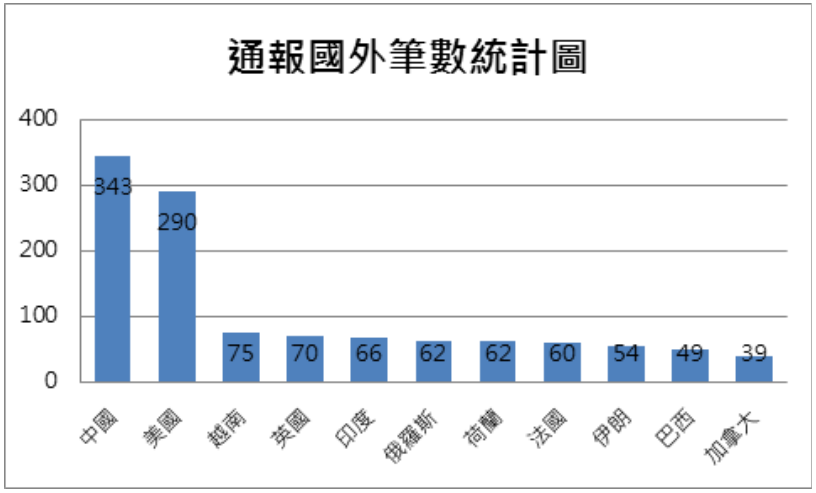

圖9 TWCERT/CC通報國外之資安事件筆數前10名

二、2017年資安通報案例

(一)Struts 2漏洞事件

2017年3月7日Apache發布公告(S2-045) Struts 2重大漏洞(CVE-2017-5638),「Struts 2.3.5 - Struts 2.3.31」以及「Struts 2.5 - Struts 2.5.10」為受影響版本,該漏洞由於Struts使用的Jakarta解析文件上傳請求包不當,當遠程攻擊者構造惡意的Content-Type可直接取得系統權限,可能導致網站資料外洩、被植入木馬程式等風險,影響機關如金融、電商、電信業等皆暴露於風險中且已有POC程式在網路流傳。

TWCERT/CC接獲緊急通報相關漏洞情資,其遭利用網址清單含政府、學術機關、民間單位總計66筆,統計如圖10。

經TWCERT/CC通報至政府資安資訊分享與分析中心(G-ISAC)並主動以電郵通知漏洞網站所屬民間機關,經查於2017年10月確認清單所列之網站皆已無Struts 2漏洞問題,Struts 2漏洞通報修正狀態統計如圖11。

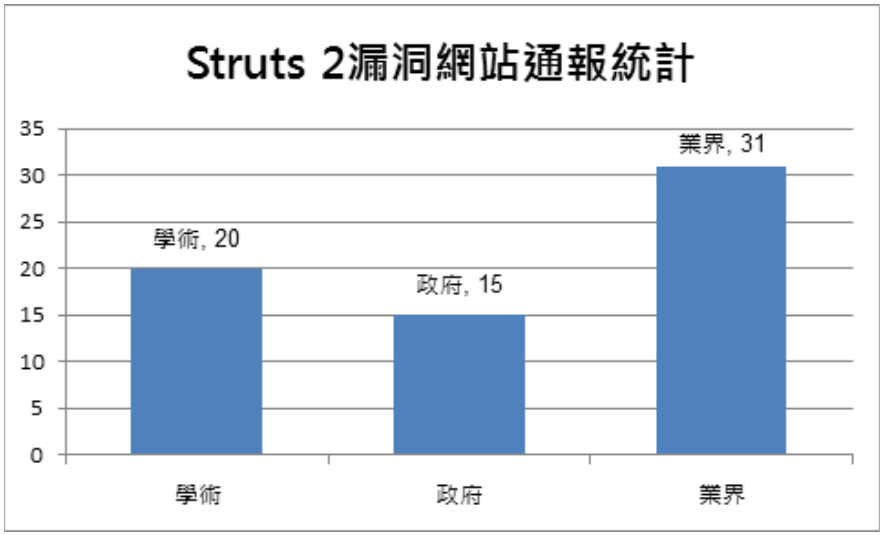

圖10 通報情資Struts 2漏洞網站統計

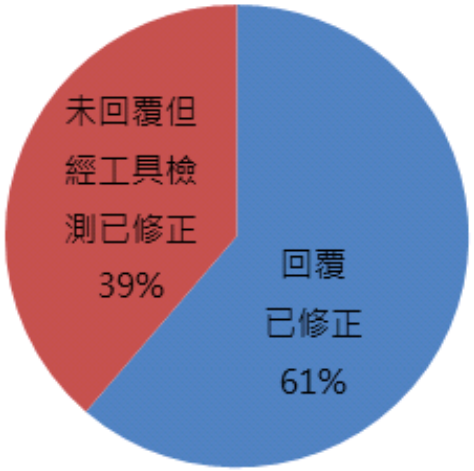

圖11 Struts 2漏洞通報修正狀態統計圖

二、2017年資安通報案例

期間也接收國內外單位通報表示遭嘗試利用Struts 2漏洞進行攻擊，攻擊次數頻繁，以國內某單位為例統計如右表。

TWCERT/CC針對Struts 2(S2-045)漏洞，提供以下幾點建議供使用Struts 2網頁框架之網站擁有者與維護人員參考：

1. 檢查系統上是否有不明程式正大量對外建立網路連線。若有則停止該程式並刪除系統上該不明程式檔案。
2. 確認網站主機是否使用Apache Struts 2的網頁應用框架，可透過檢查網站主機目錄中「WEB-INF\lib\」資料夾內的Struts2.jar檔，確認當前使用的版本。
3. 儘速更新至最新版或Struts 2.3.32或Struts 2.5.10.1版本以上。

表4 某單位通報Struts 2漏洞攻擊統計表

日期	時間	次數	國內外通報資訊
2017/03/09	06:48:44 至 06:48:57	160	國內IP
2017/03/10	21:28:55 至 21:30:12	142	中國 (ALISOFT)
2017/03/12	16:24:54 至 16:28:15	172	國內IP
2017/03/14	09:29:41 至 09:40:55	324	國內IP
2017/03/15	03:41:23 至 03:41:27	226	廣州電信 (CHINANET -GZ)

二、2017年資安通報案例

(二)網站遭轉址服務利用

TWCERT/CC接獲國內企業通報，表示他們的官方網站遭到非法轉址利用，該官方網站未經授權，遭不明人士向國內免費的網域自動轉址服務公司申請網站轉址服務，將該企業官網嵌入於免費轉址服務的網域中。以國內某旅行社為例，被利用並轉址成其它網域，如圖12及圖13。

圖12 某旅行社原本的網址及其網頁

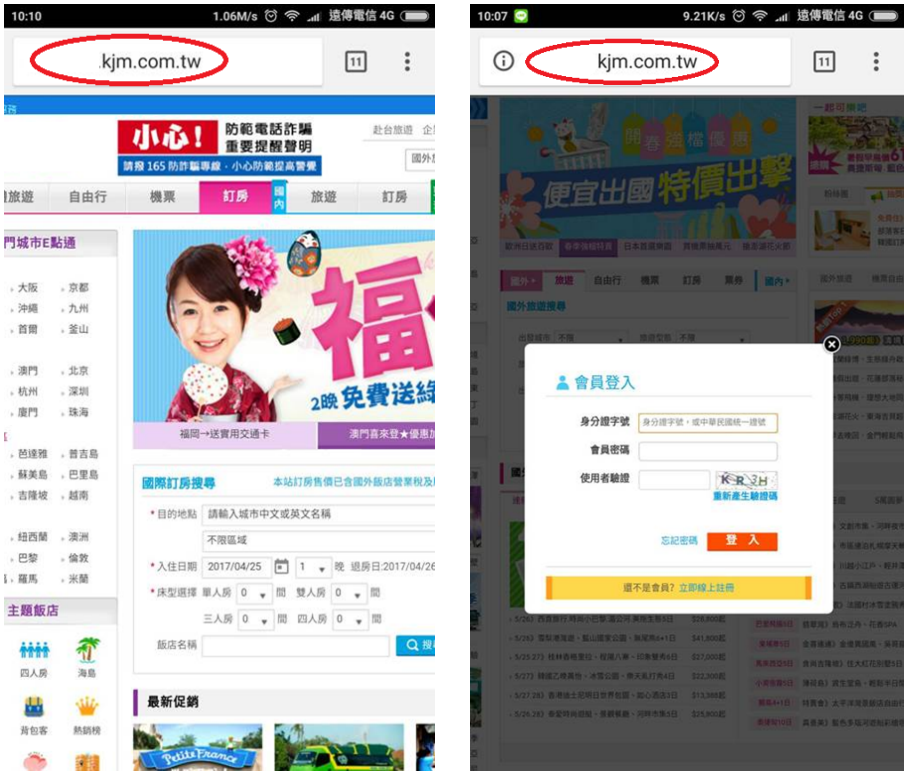

圖13 某旅行社遭偽冒網頁

二、2017年資安通報案例

除了該公司遭未授權申請網域轉址外，經查，有多達數千個網站都遭同樣手法申請網域轉址利用，其中不乏Yahoo!奇摩電影、中央通訊社等台灣民眾經常瀏覽的知名網站，遭利用的原網站網址可能被以"企業名.轉址平台名.com.tw"或"xxxxxxx.轉址平台名.com.tw"網址形式發布，例如：若企業原官網為abc.com.tw，經轉址後可能為abc.ufc.com.tw或1060711.ufc.com.tw等網址，該新的網址除內含原官網內容外，也可能會遭有心人士內嵌廣告或有害連結，來誤導使用者不小心點選連結，遭網站釣魚攻擊，如圖14所示。

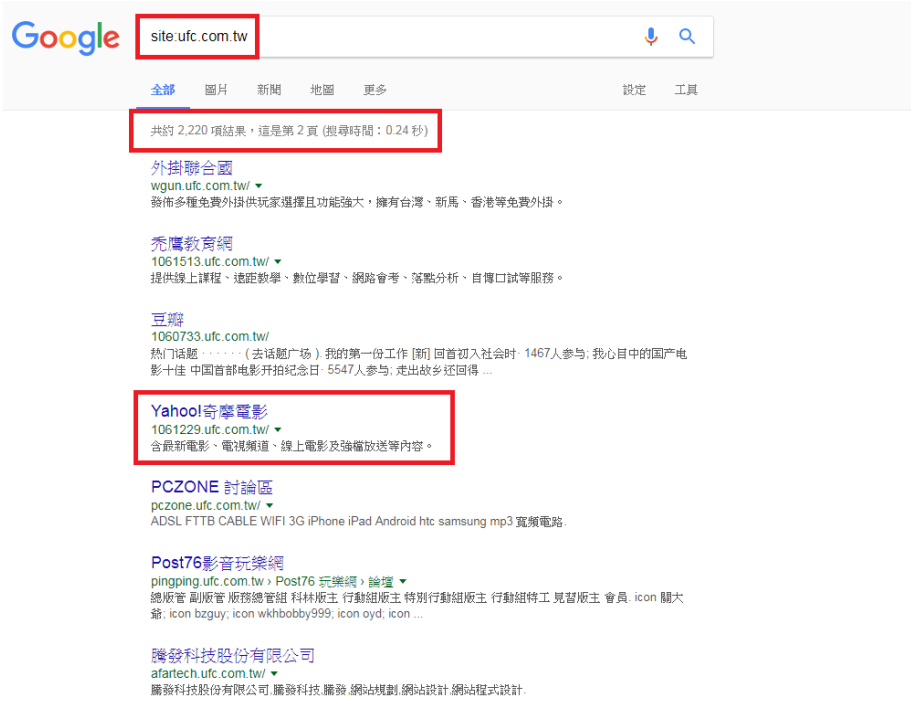

圖14 Yahoo奇摩電影網站遭利用轉址服務

網路上有許多提供免費網域轉址服務的網站，為了獲取廣告收入，針對申請者的身分認證機制並不嚴謹，有些甚至連驗證都沒有，然而有心人士可利用這樣的網域轉址服務平台，不經同意就可將知名網站加工轉換成其他網域，網站管理者通常不知道已經遭到利用做為其他用途或加入廣告頁框，如圖15。

因應近期此類利用網站知名度，非經授權申請該網站網址轉址服務，並移為它用的不正當手法，TWCERT/CC建議有以下因應措施：

二、2017年資安通報案例

1. 網站管理者應該經常以自己的網站名稱、網域等關鍵字進行搜尋，是否遭非法冒用，若發現有非網站管理者意願之重製行為，應向網域轉址服務平台反映並通報當地CERT/CSIRT組織或網域管理單位，協助移除。
2. 使用者在瀏覽網頁時，應該小心其網站名稱與網址是否有異，勿認為從搜尋引擎找到的連結都是正確的。
3. 網域轉址服務平台商應對申請者建立更嚴謹的身分驗證機制，以防止有心人士利用網域轉址服務做為網路釣魚用途。

```
<!DOCTYPE HTML PUBLIC '-//W3C//DTD HTML 4.0 Transitional//EN' 'http://www.w3.org/TR/REC-html40/loose.dtd'>
<html>
<head>
<title>[redacted]</title>
<meta name='keywords' content='[redacted]'>
<meta name='description' content=''>
<meta name='revisit-after' content='14 days'>
<meta name='robots' content=''>
</head>
<frameset rows='25,*' frameborder='NO' border='0' framespacing='0'>
<frame name='TOP_MENU' src='http://[redacted].ufc.com.tw/?PUT=ad' noresize scrolling='no'>
<frame name='MAIN' src='http://www.[redacted].com.tw'>
</frameset>
<noframes>
<body bgcolor='#FFFFFF' text='#000000'>
進入 <a href='http://www.[redacted].com.tw'>[redacted]</a>
</body>
</noframes>
</html>
```

圖15 某網站非經授權加入頁框

(三)變臉詐騙

2017年9月12日國內知名集團資訊中心通報表示遭駭客偽裝該公司某部門同仁電子郵件位址，對該公司有往來的客戶寄送帶惡意病毒程式之電子郵件，使得客戶將某筆交易之款項改匯至其它帳戶，造成該客戶的損失。經本中心協處分析後，駭侵示意圖如下圖16，以該集團提供之信件標頭(mail header)研判攻擊來自於新加坡，並將去識別化後之相關資料通報新加坡SingCERT及美國US-CERT，請求協助調查與阻檔該可疑伺服器所發郵件。

歹徒往往使用名稱非常相似的假電子郵件帳號，例如將帳號中的英文字母「l」改成數字「1」，或在帳號不顯眼處增減1字魚目混珠，甚至直接駭入企業使用的電子郵件系統，使用真正的郵件帳號發信。若匯款方沒透過第2管道查證帳戶資料是否正確，帳款就轉進了駭客的口袋，而且往往要等到真正的請款方催繳欠款，被害人才發現遇到詐騙，而匯出的款項早已被歹徒提領一空。

二、2017年資安通報案例

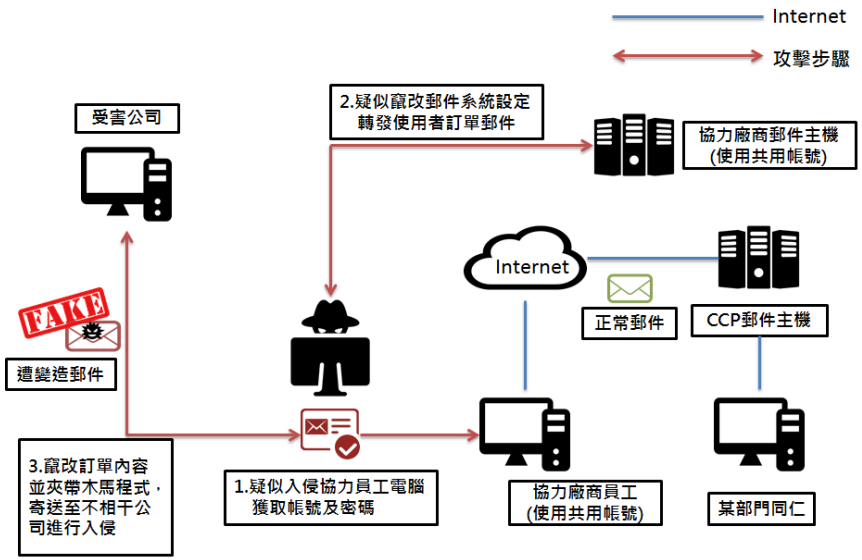

圖16 某部門信件假冒事件預測分析圖

因應近年來變臉詐騙案件不斷翻新，TWCERT/CC建議可參考趨勢科技提供給企業的6個秘訣[1]，杜絕變臉詐騙找上門：

1. 仔細檢查所有的電子郵件：小心來自高階主管的不尋常郵件，詐騙郵件最常使用簡短而含糊的主旨，有時甚至只有一個字，這些都可能為詐騙份子誘騙的動作。此外，針對要求資金轉移的電子郵件需加以確認是否為正確郵件。
2. 提升員工防詐意識：員工往往是企業資安環節中最脆弱的一環，積極做好員工訓練，仔細審視公司政策，並且培養良好的資安習慣。
3. 任何廠商變更的匯款資訊，皆必須經由公司另一位人員複核。
4. 掌握合作廠商的習慣：包括匯款的詳細資料和原因。
5. 使用電話做為雙重認證機制：透過電話撥打原本已登記的慣用電話號碼，做為雙重認證機制，而非撥打電子郵件當中提供的連絡資訊。
6. 一旦遇到任何詐騙事件，立即報警或向165反詐騙專線檢舉。

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

年度主要資安事件分析

年度主要資安事件分析

TWCERT/CC平時負責資安情資彙整及通報應變作業，此章節將針對幾個我國2017年重要的資安事件及企業較常發生的事件案例進行說明，像是網路監視器在一般家庭、工廠、辦公室、社區大樓樓梯間、大賣場等地方處處可見，網路監視器在生活中已是現代人類不可或缺的必需品，但眾多人在使用網路監視器時，並不了解資訊安全的重要性，例如時常用原廠的預設密碼或無密碼等，這些狀況都可讓駭客輕易進入網路監視器後台，隨時監控監視器的畫面，甚至遠端植入惡意程式，而成為Bot的問題。當駭客手上擁有許多Bot而形成Botnet，駭客可利用Botnet而發動DDoS攻擊。因此若網路監視器未做好相關資安設定，極有可能造成DDoS的幫兇，駭客則可利用DDoS的攻擊，而進一步進行相關錢財的勒索。

除了上述勒索方式外，在2017年中鬧得沸沸揚揚的WannaCry勒索軟體攻擊事件，透過將使用者電腦中檔案加密的方式，向使用者勒索錢財，然而即使繳付贖金，也不一定能保證檔案能復原，因此擁有基本的資訊安全認知是非常重要的。

另外，每天在收取郵件時，時常會有大量的垃圾郵件，研判電子郵件伺服器寄送大量垃圾郵件的狀況，可能是該伺服器安全性設定有疏失，例如SASL簡單認證與安全層(Simple Authentication and Security Layer)沒有設定好，SASL是提供一個以名稱及密碼來驗證用戶的機制，若您的用戶皆分散在不同網域，採用SASL認證機制則可讓您的用戶在不同網域中使用郵件伺服器寄信，甚至在同網域中寄信有使用SASL認證機制，也可提高安全性，因未經過身分認證即不能寄信。而即使有完成設定SASL認證機制，仍有可能遭駭客採用暴力破解的方式來進行攻擊。

此節將針對上述資安事件一一進行詳細分析外，在最後也將對於2017年10月國內某商銀SWIFT系統遭駭，透過偽冒交易，將巨額款項匯入駭客戶頭之事件過程及網頁遭置換攻擊事件進行詳細描述。

一、網路監視器之資安風險

英國資訊委員會辦公室(UK Information Commission's Office, ICO)警告，全球數千計之網路攝影機由於使用出廠預設的帳密而遭到破解入侵，影像遭放置於俄國網站開放全世界免費即時觀看[2]。

這些畫面多數來自家用及企業用安全監控攝影機，包括公共場合的閉路電視(CCTV)，到嬰兒監視攝影機，地點有商店、倉庫、洗手間、臥室、嬰兒室，或健身房，甚至客廳或房間。

這些被入侵的網路攝影機多半是使用廠商預設的弱密碼，像是password、12345，有的甚至未設密碼，該網站收集自世界各地之畫面，目前總數大約將近兩萬兩千台左右，包括美國近5000多則影片、日本近2000則，以及義大利和土耳其以及法國的1000多則，台灣則有300多則。

事件揭發初期，TWNCERT將該網站揭露全球攝影機遭駭情資分享於G-ISAC平台，提醒該網站會顯示台灣地區目前攝影機遭駭之情況，TWCERT/CC並開始著手透過遭公開的畫面，嘗試辨識受害使用單位，透過各方管道取得聯繫方式，將受駭攝影機相關資訊提供CCTV使用權責單位，提醒修改帳號密碼。

截至目前為止，仍有358個屬於台灣的CCTV被暴露在全世界最大的網路安全監視器網站(Insecam)上，其中Axis是個案最多的廠牌(本數據僅表示當日之廠牌統計，並不代表廠牌之資安風險性)，廠牌數量統計如圖17。

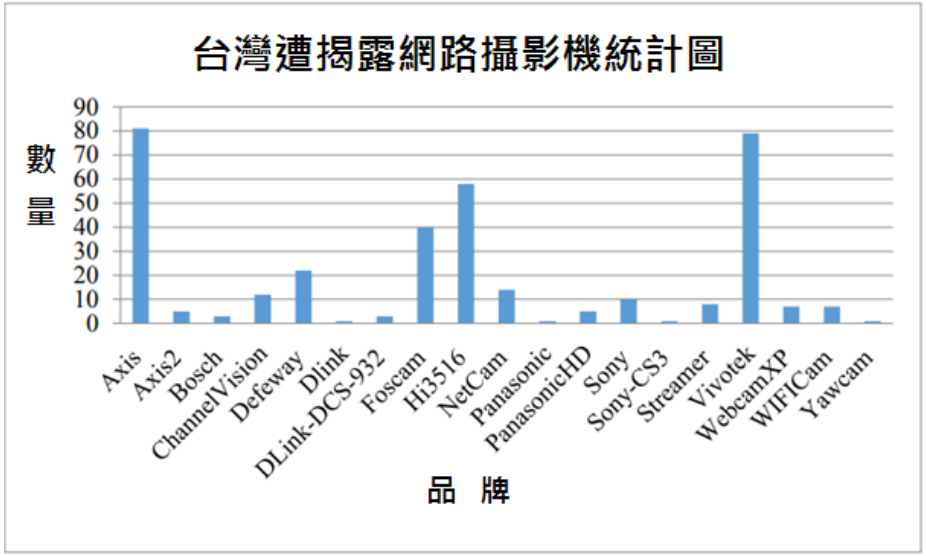

圖17 台灣遭揭露網路攝影機統計圖

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

一、網路監視器之資安風險

網路攝影機常為殭屍網路的熱門目標。而設備製造商或使用者採取的安全措施仍顯不足[3][4][5]，例如：

- 管理介面中將登入帳號密碼寫死(Hard Coding)，可能導致未經授權存取網路設備。
- 殭屍網路皆配置常見帳號和密碼組合的破解字典。大多數通常來自網路設備的預設帳號密碼。
- 由於包括CCTV在內的網路設備在安裝階段的步驟中往往缺乏適當的安全設置，因此資安專家總需要指導人們對其進行修改。
- 在CCTV / DVR設備中執行的遠端程式碼可能非常脆弱。許多設備使用BusyBox運行嵌入式Linux，這是一個包含可執行文件的常用Unix工具包。惡意軟體可以藉以掃描在BusyBox上運行的網路設備，尋找易受暴力破解字典攻擊的開放Telnet / SSH服務。

因此，為從根源避免類似攻擊情事發生，除使用者須有重設預設密碼之良好資安意識和習慣外，供應商也應該強制使用者在安裝CCTV時修改預設設定，並應在手冊中指導使用者如何修改使用者的登入帳號密碼。

然而，在網路設備尚未能更臻完善之前，TWCERT/CC建議使用者：

1. 確保存取設備的帳號和密碼已從原廠預設更改為較強之帳密組合。例如，建議包括12個字元、大寫字母、小寫字母、符號和數字。大多數設備的原廠預設帳密很容易在網路上找到，使設備暴露於危險之中。
2. 除非絕對必要，否則禁用CCTV或Web Cam上的通用即插即用(UPnP)功能[6]。
3. 監控CCTV或Web Cam上常用的IP埠，如TCP 2323 / TCP 23等，以防止遭使用Telnet協議對IoT設備進行未經授權的控制[7]。
4. 使您的CCTV和網路設備保持最新的安全修補。
5. 如非需要，應將設備設為封閉環境，僅允許區域網路使用，並關閉CCTV網路連外功能。

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

二、證券商遭DDoS攻擊勒索事件

台灣證券交易所(以下簡稱證交所)自2017年2月2日起陸續接獲國內證券商通報其入口網站/電子下單系統疑似遭分散式阻斷服務攻擊(distributed denial-of-service attack，以下簡稱DDoS事件)，部分券商表示從1月27日起陸續接獲勒索信件要求支付7到10個比特幣，隨後即遭受DDoS攻擊。

整起券商遭勒索比特幣事件可分為警告階段(1/27~2/2)、發起階段(2/3~2/8)及平息階段(2/9~)等三個階段。在警告階段，自1月27日時起國內券商陸續接收到駭客的勒索信，要求在5日內支付9個比特幣，否則券商的伺服器都將遭受高達1Tbps流量的DDoS攻擊，在接收到勒索信後，該券商的某個伺服器IP位址就遭受試探性的DDoS攻擊達15分鐘，宣示這封勒索信所言不假，並且指出若屆時限未收到贖金，勒索金額將提高至20個比特幣，每延後一日付款，贖金增加10個比特幣，而勒索信末皆自稱是「Armada Collective」的駭客組織。

案發5日後，由於券商並未妥協付款，駭客進入發起階段，隨即對券商發動DDoS攻擊，最大流量達3Gbps，進而影響正常用戶網頁下單的服務中斷，影響時間約20分鐘到1小時。攻擊手法主要為NTP(Network Time Protocol)反射放大攻擊、UDP(User Datagram Protocol) Flood及ICMP(Internet Control Message Protocol) Flood，且攻擊來源IP主要來自於海外美國。

這波攻擊事件是台灣證券期貨業者第一次集體遭受DDoS攻擊並勒索比特幣，導致網頁下單系統平均停擺半個小時，客戶無法正常透過網頁下單，但仍可採用電話或傳真方式進行交易；面對這次國內券商集體遭受勒索事件，事件從勒索到攻擊期間，並無業者支付相關贖金，截至2月13日，證交所總計接獲22件攻擊事件通報，其中共計21家證券期貨業者收到勒索信，有13家確實遭受DDoS攻擊。

二、證券商遭DDoS攻擊勒索事件

券商遭攻擊後，除啟動內部防禦機制外，亦協請ISP業者協助清洗/阻擋攻擊流量，入口網站/電子下單系統即陸續恢復正常運作。攻擊事件進入平息階段，證交所於2月9日召開「證券期貨業因應DDoS攻擊緊急應變專案小組會議」，邀集台灣期貨交易所、證券櫃檯買賣中心、中華民國證券商業同業公會、中華民國期貨業商業同業公會及電信業者等相關單位，成立DDoS攻擊緊急應變專案小組，隨時監控攻擊流量以協助券商即時應變處理，降低攻擊事件對證期市場衝擊。根據通報系統顯示，證券期貨業者網站系統除例行維修外，後續未發生大規模異常狀況，業者陸續解除通報，均指出本次攻擊事件已逐漸平息。

對於這次事件，證交所提出以下四個重點的因應措施：

表5 證交所針對證券商遭DDoS攻擊勒索提出因應措施

穩定市場	為穩定市場信心，避免不必要恐慌，金管會、證期局、行政院資安處、證交所及中華電信於期間皆曾發布新聞稿。證交所亦提醒證券商如盤中及收盤時系統有運作異常應即時通報，並由MIS系統進行公告，引導投資人改用其他方式委託。
聯繫通報	提供通報系統協助業者即時通報攻擊資訊，使相關業管單位能第一時間掌握事件訊息；並藉由資安資訊分享平台分享攻擊訊息及防護建議，以針對本次事件建立產業資安聯防。
即時監控	將開辦網路下單證券業者之官網及網頁下單網站，納入7*24小時網站監控服務，並請證券商在證交所未告知狀況解除前，每日在交易期間內於整點回報是否遭受攻擊並陳報主管機關。
防護措施	提供「證券商因應DDoS攻擊之防護及應變處置建議」，依事前準備、事中應變及事後處理分類說明相關準備措施，供業者參考辦理；並協調電信業者提供流量清洗服務，要求境外阻擋攻擊。

二、證券商遭DDoS攻擊勒索事件

台灣金融監督管理委員會對此也提出因應DDoS攻擊時，分別以事前、事中及事後三方面，提供業者以下的處置建議：

表6 金管會提供業者因應DDoS攻擊處置建議

事前準備階段	• 更新網際網路相關服務版本及關閉特定功能 • 申請流量清洗或流量分流(CDN)服務
事中應變階段	• 依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商電子交易系統故障通報機制」辦理通報事宜，同時向檢警機關報案。 • 啟用流量清洗或流量分流服務緩解攻擊，或請ISP業者阻擋來自國外之網路連線。 • 引導投資人採替代方式下單(如：電話語音下單、APP下單) • 證券期貨業者資訊人員持續協同ISP業者，監控及排除問題。
事後處理階段	• 依「證券期貨市場資通安全事件通報應變作業注意事項」進行事件解除通報。 • 記錄事件發生過程與處理程序，包含攻擊原因及手法等資訊，及因應該次DDoS攻擊採取的應變措施、解決方案與後續處理情形。

TWCERT/CC已針對DDoS攻擊勒索事件提出下列三項建議並於官方網站與官方臉書粉絲專頁提醒以下事項：

1. 建議平時與流量清洗服務業者預先擬定合作方案，俾於DDoS攻擊事件發生時可立即啟動相關機制。
2. 更新網際網路相關服務版本，升級校時系統(NTP)版本至較安全版本(如4.2.7之後的版本)，並關閉Monlist功能，避免校時系統被利用發動DDoS攻擊
3. 停用網域解析(DNS)服務的遞迴查詢功能，並設定限制網域服務回復速率(DNS RRL)，避免網域服務被利用發動DDoS放大攻擊。若業者提供服務的範圍僅在台灣地區，當DDoS攻擊事件發生時，可考慮僅允許來自台灣地區的連線，降低來自國外的攻擊造成之影響。

這類勒索手法在國際間層出不窮，業者平時應擬定因應的防護演練計畫，以降低攻擊時遭受到的衝擊。

三、勒索軟體攻擊事件與WannaCry勒索軟體行為分析

2017年5月12日，全球傳出大量遭WannaCry勒索軟體攻擊之災情，網路資安公司發現全球多個國家的機構及個人電腦遭受名為「WanaCrypt0r 2.0」的勒索軟體攻擊感染，有別於以往的攻擊方式，該勒索軟體是直接透過系統漏洞進行攻擊，除Windows 10及Server 2016外，近乎所有Windows系統及其伺服器版本均受威脅，資安專家即呼籲必須安裝官方釋出的安全性更新，以避免機構及個人電腦受感染。

此勒索軟體的運作模式一如既往，電腦遭受感染後，所有檔案均被加密成副檔名為.WNCRY的格式，無法正常開啟讀取資料。檔案加密後亦會彈出相應介面指示受害者需在3天內交付價值300美元的Bitcoin贖金，逾期加倍，若未能在7天內交付則再也無法恢復檔案。

「WanaCrypt0r 2.0」是透過Windows系統內名為EternalBlue的Windows SMB遠端執行程式碼弱點進行攻擊，成功利用弱點的攻擊者有機會獲得在目標伺服器上執行程式碼的能力，不用點擊網頁，受害設備連上網路就會中毒，導致檔案被加密勒索[8]。

WannaCry勒索軟體行為摘要[9]：

- WannaCry軟體(主程式名稱mssecsvc.exe)之MD5雜湊值為DB349B97C37D22F5EA1D1841E3C89EB4，執行後會創建四個檔案tasksche.exe、Taskdl.exe、@WanaDecryptor@.exe、Taskse.exe。
- 主程式mssecsvc.exe於執行期間，具大量對外連線445網路埠行為，嘗試進行本體擴散。
- tasksche.exe程式會先針對檔案進行加密，再刪除原檔案，並新增原檔同大小檔案企圖覆蓋原檔案位置(嘗試對被刪檔案進行救援作為，可成功救回部分遭刪檔案)。
- @WanaDecryptor@.exe程式會執行機碼寫入作業，位置為 REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\emxsssho787，旨提供該軟體可隨電腦系統重開機時自動執行之。
- @WanaDecryptor@.exe程式亦會對外連線，其中包含利用Tor機制匿蹤來源。

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

三、勒索軟體攻擊事件與WannaCry勒索軟體行為分析

主程式mssecsvc.exe等五個行程執行關聯如下圖18：

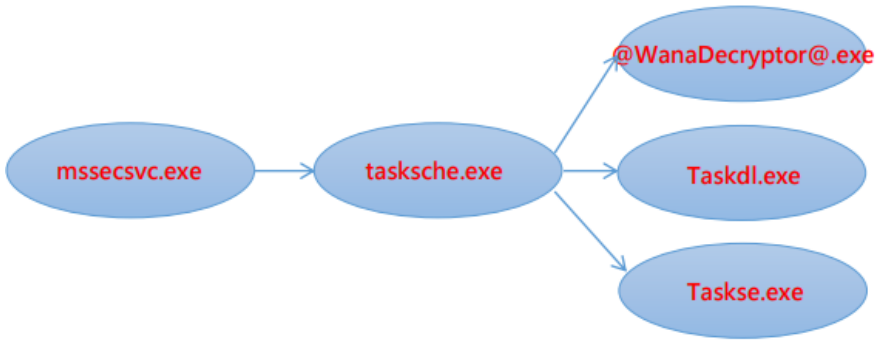

圖18 主程式mssecsvc.exe等五個行程執行關聯圖

後續TWCERT/CC收到國內某單位請求，表示其單位行政電腦遭受勒索軟體感染，並於5月22日前往該單位進行事件調查及作業環境等訪談，取得該單位同意後進行採樣分析，並取回硬碟複本。發現WannaCry病毒母體mssecsvc.exe植入時間為2017/05/22 03:27:22，第一個被加密檔案時間為2017/05/22 03:28:07。在檔案受駭情形方面，C磁區被加密檔案數量共計350,882個，D磁區被加密檔案數量共計426個，合計351,308個檔案。在檔案回復情形方面，使用檔案磁碟救援軟體回復磁碟中被刪除檔案，經統計共回復C磁區檔案698,303個(160.33GB)，D磁區檔案2,984個(73.81GB)，共計701,287個檔案，所回復之檔案中，部分檔案為原使用者遭勒索加密前所刪除之檔案，因此回復數量大於被加密的檔案數量，全磁碟救援共耗25小時，藉由本次現地資安事件處理成功，使得民間對TWCERT/CC有更為加深之認識與信任。

三、勒索軟體攻擊事件與WannaCry勒索軟體行為分析

針對WannaCry勒索軟體，TWCERT/CC提出以下應變作為：

1. 確認電腦無法連上網路，使用有線網路者拔除網路線，使用無線網路者亦須確保無法連上網路(例如關閉Wifi分享器電源或拔除3/4G無線網卡)。
2. 將電腦開機進到安全模式(大部分電腦在Windows畫面出現前長按F8即可進入安全模式選單)，或透過外接安全的系統進行開機。
    a. 將重要資料複製到外接式硬碟(備份完請記得將外接硬碟拔除！)。
    b. 若尚未安裝修補程式者，請依照作業系統版本安裝適合的修補程式，可連上網路下載修補程式，或使用隨身碟把檔案移至電腦內。
    c. 斷網並重新開機進到一般模式後安裝修補檔。
3. 若電腦開機進入一般模式，出現疑似中勒索軟體現象(如桌面檔案出現異常無法打開)，即刻拔除電源或關機(使用筆電者請亦將筆電電池移除)，並確認電腦無法連上網路，使用有線網路者拔除網路線，使用無線網路者亦須確保無法連上網路(例如關閉Wifi分享器電源或拔除3/4G無線網卡)。

後續處置作法：

a. 未被加密的重要資料備份：使用安全模式開機或透過外接安全的系統進行開機，將還尚未被加密的重要資料複製到外接式硬碟(被加密的檔案目前還尚未有任何解密方法)。
b. 系統恢復：將受駭電腦硬碟格式化後重灌至最新版官方作業系統。

4. 若無中勒索軟體現象，即刻將重要資料備份，備份資料離線保管。若要確認是否有感染，可搜尋磁碟中是否有.wncry附檔名檔案，若有或疑似已中WanaCrypt0r 2.0病毒，續照步驟3方式處理；若無則可能尚未中毒。
5. 若電腦中原無安裝防毒軟體，可下載微軟官方所提供之防毒軟體Windows Defender，可針對系統中的惡意程式WannaCryptor提供偵測並清除。Windows Defender下載位置: https://support.microsoft.com/zh-tw/help/14210/security-essentials-download
6. 隨時更新修補程式及防毒軟體至最新版本，使用防火牆並關閉不需要之通訊埠及應用程式權限，以確保電腦安全無虞，不要因為一時方便開啟不必要的服務，而導致系統出現漏洞。另對防火牆及IDS/IPS等設定部份，建議設定可阻擋WannaCry所使用MS17-010漏洞之特徵或規則。

四、SASL認證暴力破解攻擊事件

TWCERT/CC接獲通報得知：某單位2017年4月起持續遭國外以特定模式進行網路攻擊，經分析攻擊來源截至6月底約84%比例皆來自中國IP，由通報者提供之伺服器紀錄發現，攻擊手法皆屬嘗試暴力破解SASL認證之方式攻擊郵件伺服器。

所謂SASL為簡單認證與安全層(Simple Authentication and Security Layer)，一種在既有網路協定中認證機制的框架與標準，規範了客戶端與服務應用間的認證和可選之安全層的建立，定義如何交互認證資料，沒有限定資料內容，使用SASL程式協定，理論上即可支援SASL所有的認證機制。

在郵件伺服器中，SMTP(Simple Mail Transfer Protocol)初始設計並未將身分驗證部分考慮進去，且透過符合郵件伺服器中的轉寄(Relay)設定，雖可以在區域網路內經由郵件伺服器送信，但使用者不在轉寄(Relay)設定範圍時，則必須有認證機制以避免成為垃圾郵件(Spam Mail)的開放式轉寄(Open Relay)，SASL則為一種管理POP、IMAP或SMTP用戶端向伺服器證實自己身分時所廣泛使用之機制。

該單位於2017年3月底前通報遭受攻擊之來源國家大多分散且攻擊模式不一，然而至2017年4月初起，除其他常見通報之攻擊模式外，開始出現一種特定攻擊模式，每次通報之IP數異常大量，經檢視發現為不明IP高密集的嘗試暴力破解SASL認證模式，攻擊該單位之郵件伺服器。該單位所提供之伺服器紀錄如下：

Jul 9 18:39:47 mail postfix/smtpd[xxxx]: warning: unknown[xxx.xxx.xxx.xxx]: SASL LOGIN authentication failed: authentication

四、SASL認證暴力破解攻擊事件

此攻擊模式持續至今尚未停止，且成為該單位通報之大宗案件，經彙整2017年4月至6月止之通報案件中針對該攻擊模式所提供之伺服器紀錄統計分析後，攻擊來源分別來自49個不同國家，攻擊IP數總計有1001筆，所屬國家為中國之比例為最大宗，共計835筆IP數，二、三名分別為美國38筆、越南及印度13筆，落差相當懸殊，其他45個國家則為個位數，來自中國之IP占全總數84%，如圖19所示。

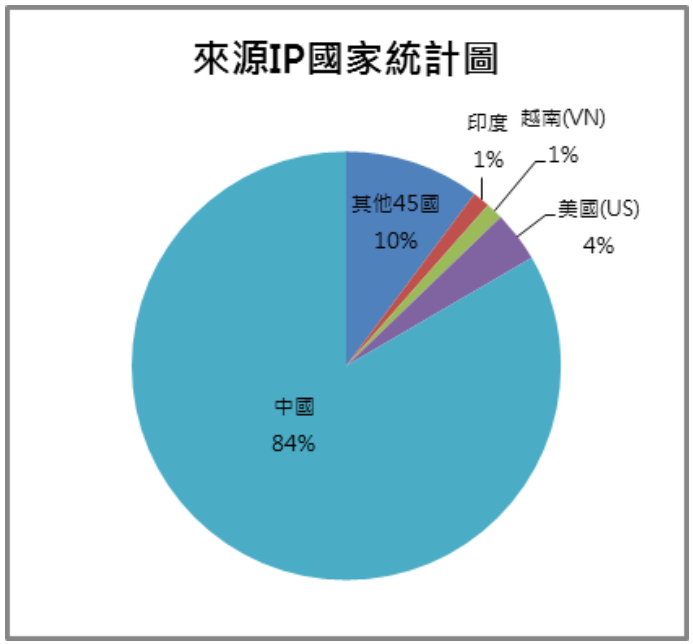

圖19 來源IP國家統計圖

針對國際間對郵件伺服器攻擊活動相當頻繁，當郵件伺服器遭侵入被駭客掌握時，後續所衍生的惡意行為諸如冒名郵件、垃圾郵件(Spam Mail)、自動執行勒索軟體附件(Ransomware attachments)等將大量發生，若再以蠕蟲主動擴散至電腦主機(Personal Computer)甚至企業主要伺服器，將可進行計畫性大規模攻擊，因此郵件伺服器常被利用為主要侵入突破點，應列為各單位重要之資訊資產，並嚴加防護。

四、SASL認證暴力破解攻擊事件

因應此類攻擊活動，TWCERT/CC建議應有以下措施：

1. 立即檢視郵件伺服器相關活動日誌，查詢是否有曾遭受類似攻擊紀錄。
2. 定時更新軟體、韌體修補，以防出現零時漏洞遭駭客利用。
3. 定期更換管理者(root)密碼，並適當增加密碼強度，以避免遭暴力破解。
4. 強化安全防護設定，如限制信件代轉設定、郵件過濾機制、郵件管制臨界值等設置。
5. 使用防暴力破解工具(如Fail2Ban等)來防止有心人士暴力破解SASL認證及防範Linux伺服器上的SSH、vsftp、dovecot等服務免於遭駭客使用暴力密碼入侵[10]。

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

五、國內某商銀SWIFT系統遭駭事件

國內某商業銀行內網遭駭客入侵植入惡意程式，並偽冒SWIFT交易，將巨額款項匯往斯里蘭卡、柬埔寨、美國等國的駭客帳戶中，金管會檢查局及資訊服務處派員調查後發現，本資安事件疑似為APT攻擊手法。

經相關單位調查分析後，本案惡意程式包含散布、加密、遠端遙控等功能[11]，在駭入內網後，再感染個人電腦與伺服器，駭客透過遠端控制惡意程式，將蒐集到的國內某商銀系統資料，傳送至位於美國及荷蘭的C&C伺服器(Command and Control Server)。惡意程式另以加密國內某商銀系統資料方式進行證據破壞，並讓受駭者誤認為此事件為勒索軟體攻擊，使得某商銀作業人員第一時間沒發現SWIFT系統出現異常交易，避免被追查，駭客更利用受駭者較疏於防範的假期來發動攻擊，最後成功偽造七筆匯款電文，共匯出六千多萬美元。

駭客掌握了整個SWIFT交易方式與該銀行運作，經分析研判，整起事件之攻擊源疑似來自魚叉式釣魚郵件，又因SWIFT系統並未落實實體隔離，使得駭客可以成功入侵。TWCERT/CC提醒企業務必重新檢視單位內系統的權限管控與實體隔離機制是否澈底實施。

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

五、國內某商銀SWIFT系統遭駭事件

經調查發現駭客犯案手法是透過寄送電子郵件給特定銀行職員，利用釣魚郵件進行惡意程式布建後，再由惡意程式駭入內網進行SWIFT系統攻擊與勒索軟體加密攻擊，其所使用之針對性攻擊手法如下及圖20所示[12]。

- 駭入某商銀SWIFT系統，取得某商銀SWIFT系統轉帳憑證。
- 偽冒受款對象及金額等交易資料並以電文發送。
- 透過中介銀行轉到駭客指定的銀行帳戶。
- 對方銀行收到電文後會把款項撥到指定帳戶內，造成盜轉。
- 加密某商銀電腦資料，混淆某商銀資訊人員事件處理焦點。

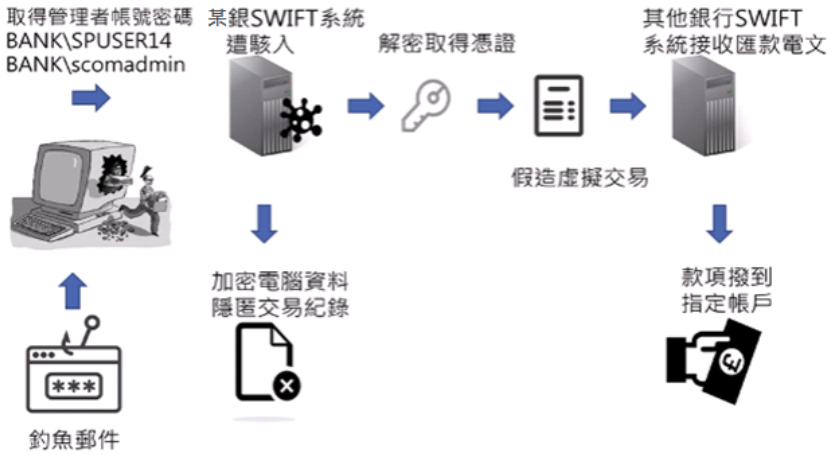

圖20 國內某商銀SWIFT系統遭駭手法

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

五、國內某商銀SWIFT系統遭駭事件

針對此次某商銀遭駭事件，引用金管會所提建議的參考文獻包括健全交易審核機制、加強整體資安結構並強化人員資安教育、厲行資安防護作為及防堵駭侵事件擴大等4項要求與建議[13][14][15]。

TWCERT/CC於事件發生後於10月6日第一時間即在Facebook粉絲專頁上發布金管會新聞稿等情資，供企業及民眾參考，並於10月7日將相關情資分享予APCERT(亞太地區電腦網路危機處理中心)。企業除應照金管會提出之要求建議強化APT防護機制，以防堵是類事件再次發生外，針對此事件的攻擊手法，TWCERT/CC亦提醒企業須注意下列事項，以防類似攻擊事件的發生。

1. 企業需重新檢視實體隔離網路架構，是否嚴格落實隔離機制，並所有可連線的設備均須納入企業風險評估的範圍。
2. 系統存取之權限控管務必要落實，且必須針對重要系統有完善的監控機制，當異常連線發生時須即時發出警訊告知管理者，並小心使用特權帳號，當授權時效過後，應馬上將特權帳號移除。
3. DDoS或勒索病毒攻擊有可能是駭客目標式攻擊的前置作業，當企業遭受DDoS或勒索病毒危害時，須同時檢查單位重要系統，注意系統是否有無其他非法存取之異常現象，以避免聲東擊西之攻擊手法。
4. 企業應加強宣導並要求使用者於使用電子郵件時，務必確認郵件真偽，且不隨意開啟附件與網路連結，以避免釣魚郵件。

企業應建立資安事件處理小組(Computer Security Incident Response Team, CSIRT)與事件處理程序，並宣導讓員工了解當發生資安事件時的通報協處管道，以加速資安事件處理時效。

註：點擊引用編號可連結到參考資料頁；點擊參考資料頁之引用編號可返回原文頁。

六、網頁遭置換攻擊事件

網頁置換(Defacement)是一種網頁攻擊，一般攻擊方式為駭客入侵受害網頁伺服器並將受害設備之原網頁替換成其它駭客自製的網頁，常見於有政治動機的「網路抗議者」、激進駭客用來傳播訊息或是用以炫耀技術、戰績，例如知名的網頁置換揭露平台zone-h，擁有大量國際駭客所分享之成功攻陷並置換的網頁快照資料庫，遭到網頁置換之主因通常為網站或伺服器設備出現漏洞，因此遭駭客入侵與控制。

TWCERT/CC於2017年初即開始關注台灣地區遭公布於zone-h上受駭網頁的情資，並將結果通報相關負責單位修訂，至2017年12月22日，zone-h網頁置換揭露平台資料庫中遭置換網頁之受害網域屬「.tw」者，總計有39,264組，其中不重複之IP計有16,575 組，且有22,689組為單一伺服器上之其他網頁被入侵，這常發生在虛擬網站伺服器上，只要單一的服務出現漏洞，整個伺服器上之網頁都可能受害，如下圖21。

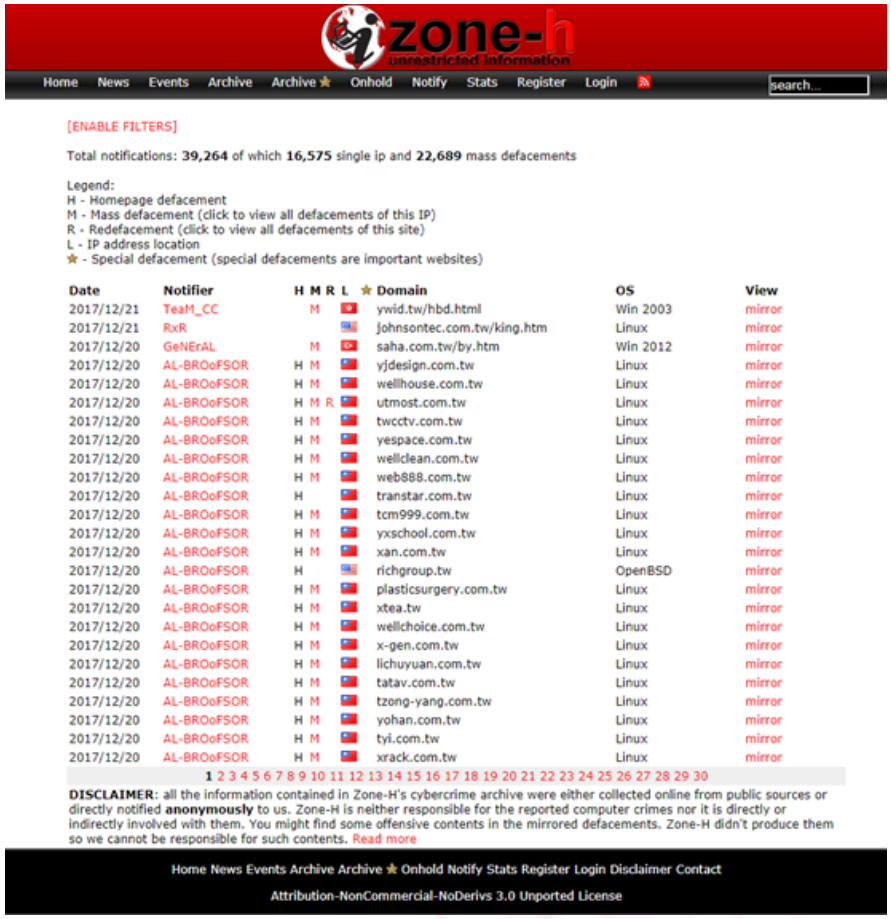

圖21 zone-h網頁置換揭露平台以「.tw」搜尋條件結果畫面(2017/12/22)

六、網頁遭置換攻擊事件

然而網頁置換攻擊表面上看來只是駭客單純的惡意行為，但背後真正的問題在於網頁伺服器既然能被駭客侵入，就有可能被置換成為釣魚網頁、植入後門或惡意跳轉程式，駭客可以透過釣魚網頁連結，引誘一般使用者訪問看起來和受害網站相仿，或甚至看似為其他網路服務的特製網頁，並要求他們提供私人資訊，導致使用者受騙或遭利用，而一旦受害網站被認定為具有網路釣魚的網站，便可能遭防毒軟體或防火牆系統將其列入黑名單，致使受害單位網站遭受牽連，造成單位業務推展不利甚至信譽受損進而影響商業利益等情事。

TWCERT/CC經分析這些紀錄，通報IP重複出現一次以上之資料，並篩選出該資料之通報來源同時包含zone-h揭露平台及其他單位之紀錄共計18組，並與通報紀錄中常見的釣魚網站通報單位Phishlabs及Netcraft對照分析統計如下表及下圖22所示。

表7 重複通報IP包含zone-h及其他通報單位統計表

重複通報 IP 包含 zone-h 及其他通報單位統計表			
	單位	IP 組數	事由
常見通報單位	Phishlabs	6	釣魚網頁
	Netcraft	4	釣魚網頁
同時包含 Phishlabs 及 Netcraft	Phishlabs 及 Netcraft	2	釣魚網頁
			釣魚網頁
	法國 CERT	2	釣魚網頁
	美國資安公司		釣魚網頁
其他	HITCON ZeroDay	4	網頁弱點
	芬蘭 CERT		釣魚網頁
	巴西 CERT		釣魚網頁
	TWCERT/CC		網頁資料洩漏

六、網頁遭置換攻擊事件

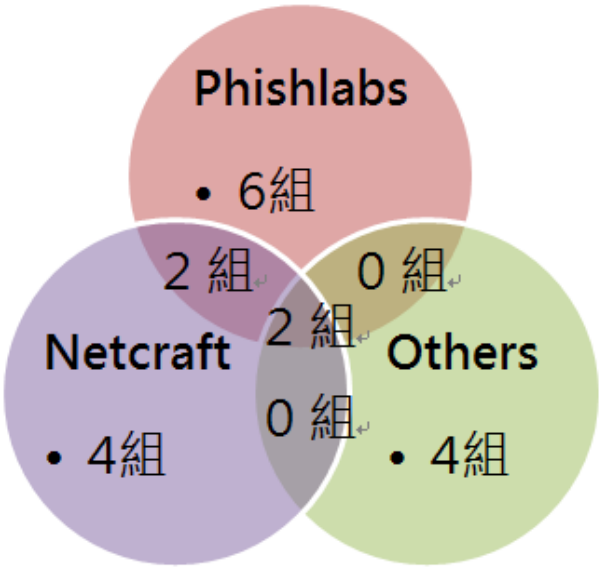

圖22 重複通報IP包含zone-h及其他通報單位統計

分析後發現，重複通報之IP有出現在zone-h且有其他單位通報之紀錄者，皆為網頁問題類型之通報，如網頁出現弱點遭HITCON ZeroDay揭露、TWCERT/CC通報應變小組人員發現網頁機敏資訊外洩，以及TWCERT/CC國外固定合作夥伴Phishlabs和Netcraft及其他國家CERT或資安公司所通報之釣魚網頁。

由此證明，當網頁遭揭露於zone-h網頁置換平台時，確實有可能發生前述之背後隱憂，因此網站擁有者或維護者應將網頁置換攻擊視為警鐘，系統可能存在允許駭客變更網站資料的嚴重漏洞，若引發其他更多或更嚴重之入侵攻擊之情事，損失將會更大，企業如發現網頁遭置換應全盤檢視系統安全，並強化防護作為，否則如置之不理而遭植入惡意程式或連結而成為釣魚網頁，將會成為網路犯罪的共犯。

網站擁有者或維護者往往認為網站系統已經安裝最新的修補程式不會有弱點，然而系統漏洞與Web應用程式漏洞是不同層面，網頁的安全性僅僅只是整體系統安全的其中一環，因此針對網站安全防護，TWCERT/CC區分系統防護以及網頁應用安全部分提出以下建議。

六、網頁遭置換攻擊事件

I. 系統防護建議：

1. 網站伺服器的作業系統及應用程式務必安裝最新版的安全更新，並定期進行弱點掃瞄。
2. 安裝防火牆以及防毒軟體，並正確設定防火牆規則，保持防毒軟體掃毒引擎與病毒碼更新至最新。
3. 關閉不必要之網路服務，建立密碼時使用複雜度高之強密碼規則。

II. 網頁應用安全建議：

1. 網站開發時，應要求開發商納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC)。
2. 網站上線後，應定期檢視網站建置環境及所使用之套件以及外掛程式等所屬廠商之更新支援狀況，並保持最新；如發現廠商公布不再支援更新修補，應即檢討可用性以及替換方案。
3. 當上線的網頁發生問題時(如遭置換網頁或被通報有弱點)，應即時修補相關弱點，全面檢視全系統的安全，並監控相關活動紀錄，以確認無其它的攻擊或惡意程式植入情事。

TWCERT/CC將持續觀察網路上各資安情資平台，挖掘與台灣相關之攻擊或受害資訊並通報受害或權責單位即時進行應變處理，透過蒐整之情資分析研判資安趨勢，達到可向國際相關單位發布威脅預警情資之目標。

情資交換平台TWCERT-ISAC

情資交換平台TWCERT-ISAC

目前各資安組織皆陸續建置情資交換平台ISAC，為了即時掌握最新資安情資，TWCERT/CC規劃開發TWCERT-ISAC平台，透過此平台與其他資安組織ISAC進行界接，以自動化的方式交換情資，促進資安事件處理效率，以達到國際資安聯防之目的。TWCERT-ISAC之功能包括：「自動化資安通報系統、資安通報工單系統、惡意樣本檢測平台(MARS)、資安資源庫系統、威脅預警系統，及情資分享平台。」以下將針對TWCERT-ISAC平台規劃內容及前三項功能依序介紹。

一、情資交換平台(ISAC)

本中心扮演國際與國內資安事件處理的協調角色，與國內外資安組織緊密聯繫與合作，加速事件協調與處理時效，提升整體資安聯防與應變能力。因應數量日趨成長之資安事件及情資，人工作業已無法滿足作業所需，因此，本中心規劃開發及建置TWCERT-ISAC平台，藉以提升業務品質及效率。TWCERT-ISAC平台架構如下圖23。

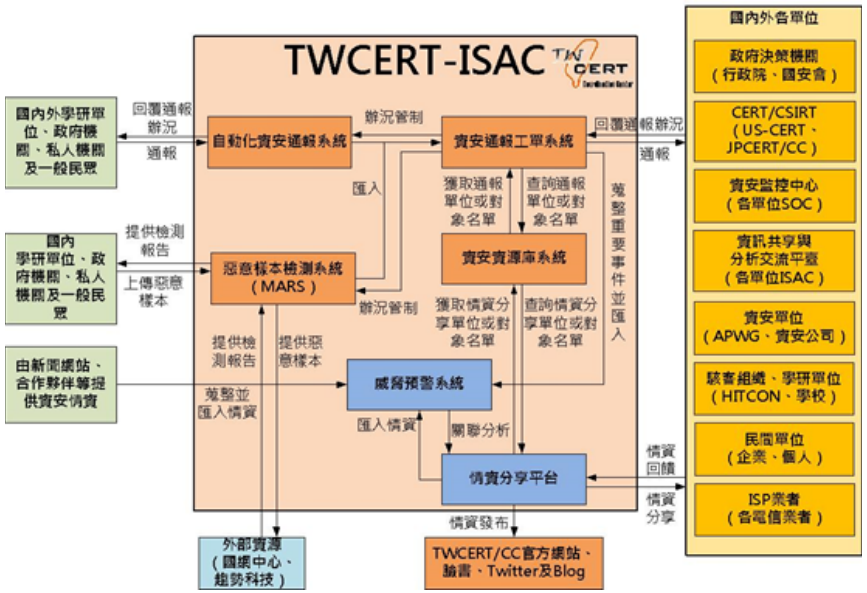

圖23 TWCERT-ISAC平台架構

二、惡意樣本檢測系統(MARS)

為避免國人將含有機敏資訊之樣本誤傳至國外樣本檢測系統中，本中心設計一網頁介面，供民眾及各單位上傳惡意樣本，並可查詢檢測進度，本系統之樣本係送至財團法人國家實驗研究院國家高速網路與計算中心(以下簡稱國網中心)進行檢測後，透過此系統產出程式行為檢測報告提供給檔案上傳者參考。

長期經營此系統，預期可建立台灣特有惡意樣本資料庫及掌握台灣網路遭駭侵現況，除分析台灣特有之駭侵行為及未來駭侵趨勢外，同時也可避免國人將含有機敏資訊之樣本誤傳至國外樣本檢測系統中，導致我國機敏資訊外洩(惡意樣本檢測系統介面如圖24及圖25)。

依行政院資通安全處指導規劃，此系統第一階段提供政府機關使用，第二階段將提供關鍵基礎設施提供者、公營事業及政府捐補助之財團法人等，最後在系統漸趨穩定後，將會開放給全國民眾使用。

二、惡意樣本檢測系統(MARS)

圖24 惡意樣本檢測系統介面-1

圖25 惡意樣本檢測系統介面-2

二、惡意樣本檢測系統(MARS)

此系統英文名稱為Malware Analysis and Report System, 簡稱為MARS, 為本中心與國網中心共同開發, 其開發時程如圖26所示並已於2017年8月16日完成系統上線, 並由行政院資通安全處函請各政府機關使用, 統計至12月31日總造訪人數(不重複)已達4,184人, 完成674筆樣本檢測, 其中614筆檢測出低風險、38筆檢測出中風險、22筆檢測出高風險(統計如圖27)。

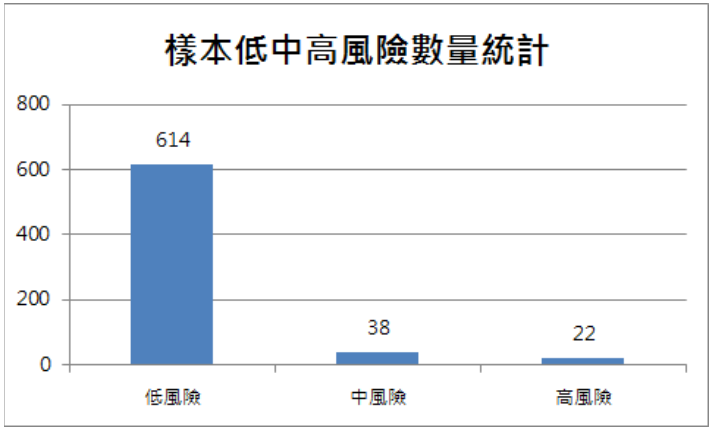

圖27 樣本低中高風險數量統計

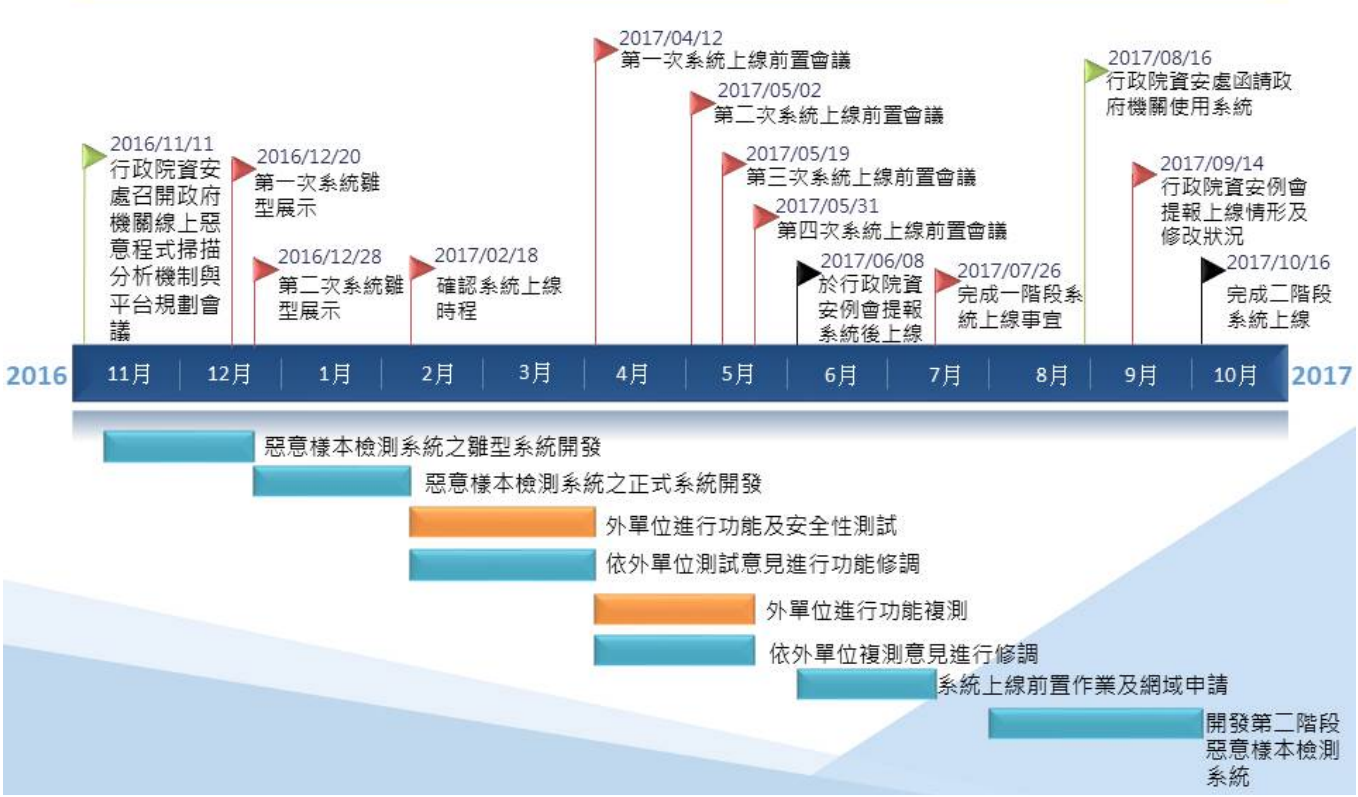

圖26 惡意樣本檢測系統開發時程

三、自動化資安通報系統

自動化資安通報系統的目的為以標準化介面，供民眾及各單位通報資安事件，查詢事件處置進度及給予相關處置建議。使用標準化通報介面將有利於後續與國內外各單位界接，加速通報流程。目前提供使用者透過友善網頁介面及API通報資安事件及查詢處置進度，標準化API通報有利與國內外各單位自動化通報系統介接，加速通報流程並便於追蹤，友善網頁通報介面有利於提升民眾通報資安事件意願等效益(自動化資安通報系統介面如圖28及圖29)，目前亦可由TWCERT/CC官網之資安通報選項中進行通報。

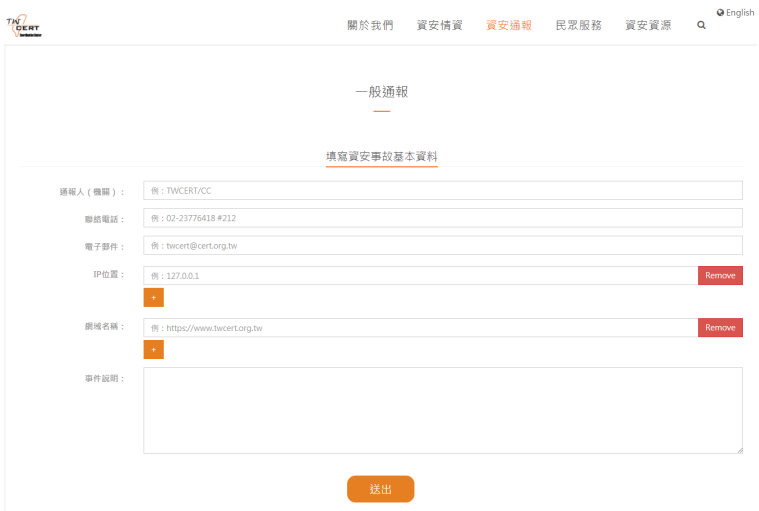

圖28 自動化資安通報系統介面-1

圖29 自動化資安通報系統介面-2

四、資安通報工單系統

透過資安事件標準編號之建立，來進行資安事件記錄、追蹤、研判與分級等作業，本中心開發資安通報工單系統，有利於通報事件辦況管制並掌握全球資安事件趨勢，以分析駭客行為及未來駭侵事件趨勢(資安通報工單系統介面如圖30及圖31)。

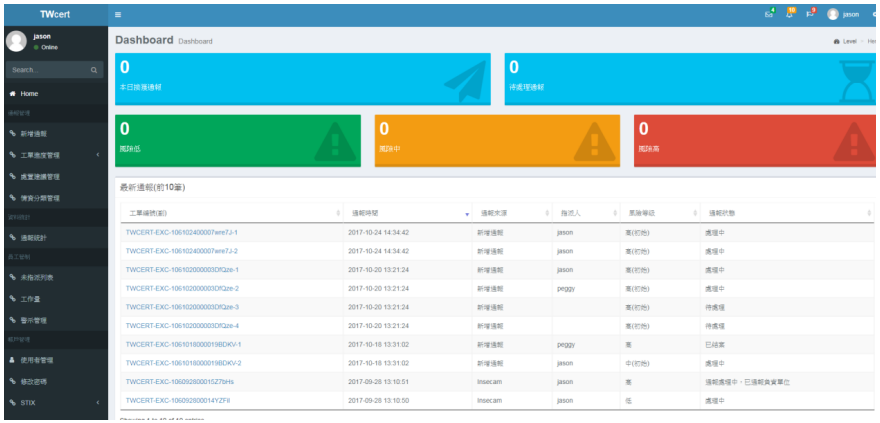

圖30 資安通報工單系統介面-1

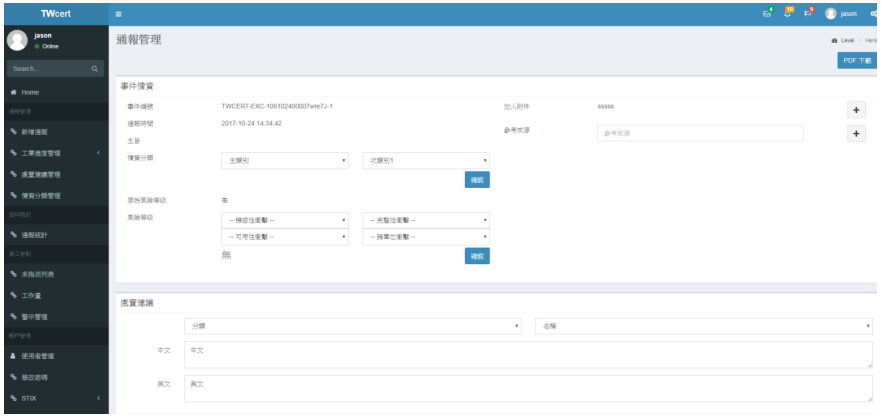

圖31 資安通報工單系統介面-2

合作交流與會議活動

合作交流與會議活動

TWCERT/CC平時也積極與國際資安組織協同合作，目前為FIRST資安事件應變小組論壇(Forum of Incident Response and Security Teams)及APCERT亞太區電腦緊急事件回應小組(Asia Pacific Computer Emergency Response Team)會員，定期參與每年舉辦的盛大年會，透過參與年會的方式了解各CERT/CSIRT的執行狀況及近期所探討的熱門資安議題，平時也積極與這兩大國際資安組織密切交流，互助合作，定期參與線上演練作業，以提升及確保該成員的資安事件應變能量。 除此之外，TWCERT/CC於2017年也與台灣CERT/CSIRT聯盟成員合作舉辦2017年台灣資安通報應變年會，針對資安通報應變進行宣導，希望聽眾能對資安通報應變有更進一步的認識，藉以提升資安通報意願，並了解事件處理流程的方法及步驟。

一、國際資安組織交流現況

(一)參與國際重要會議

2017年3月15日至16日赴馬來西亞參與第五屆亞洲地區情報(Cyber Intelligence Asia)會議，於會中介紹TWCERT/CC及分享台灣地區資安事件案例，並與馬來西亞(MyCERT)、泰國(ThaiCERT)、印度尼西亞(ID-CERT)等國家CERT進行交流，有效掌握亞太區最新資安趨勢、防護技術及資安政策與戰略，除推展本中心之知名度，也藉此對於維護亞太區資安環境發展有所貢獻。

2017年6月11日至16日赴美國波多黎各參加第29屆資安事件緊急應變小組論壇年會(29th Forum of Incident Response and Security Teams Conference)，計有全球超過70個國家的會員單位與會，其研討會內容包含網路威脅型態變化、資安事件處置與現地處理、網路威脅情資平台、惡意程式分析與檢測等，本次年會主軸為「Fighting Pirates and Privateers」，著重於網路攻擊事件無國界之分，各國通報應變人員應強化情報活動(Intelligence Activities)相關作為，各國之間應持續不斷地相互合作與情報分享，會員應協助國際電腦資安事件處理，並即時分享資安威脅情資及共同打擊網路威脅事件。

圖32 TWCERT/CC主任陳永佳赴馬來西亞參與第五屆亞洲地區情報會議

一、國際資安組織交流現況

2017年11月11日至16日赴印度新德里參加2017年度亞太區電腦事件應變小組年度會議及研討會(APCERT Annual Gerneral Meeting & Conference 2017)。會中與各國資安組織交流資安預警情資、研討國際CERT/CSIRT資訊通報經驗及蒐集資安防護與通報應變作法，共同推動國際網路安全交流合作及資安事件協處支援。藉由參與本次會議，汲取國際及業界資安科技新知，亦掌握新型態之資安威脅態樣及數位鑑識技術，以提升資訊安全應變處置能力，進而強化整體資安能量。會中亦發表我國惡意樣本檢測系統介紹(Malware Analysis Platform in Taiwan- MARS)，除推展本中心之知名度，也藉此推廣我國於整體資安防護之努力，及對於維護亞太區資安環境發展有所貢獻。會中各國CERT也贊同此系統之開發概念，並認同此為各國需重視議題，此外，澳洲AusCERT亦於參與APCERT後，於官方部落格中提及此次我方所發表議題(網址： https://www.auscert.org.au/blog/2017-11-17-apcert-2017-agm-and-conference-window-c)。

圖33 TWCERT/CC分析師羅文翎赴印度新德里參加APCERT 2017年會

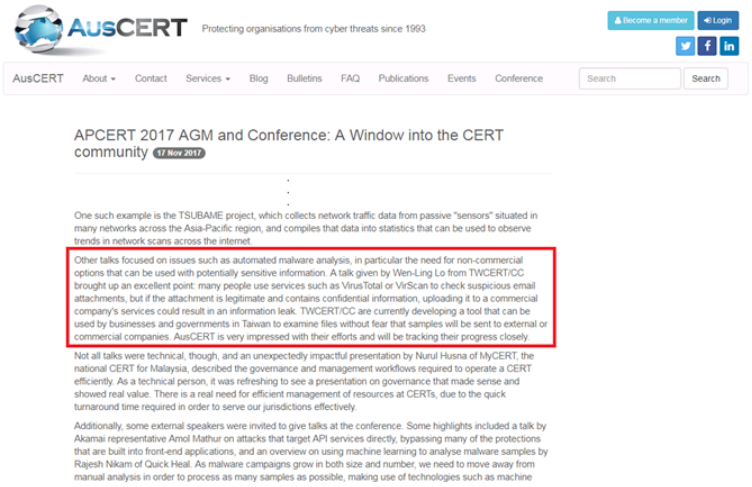

圖34 澳洲AusCERT於官方部落格中提及此次TWCERT/CC發表議題

一、國際資安組織交流現況

(二)參與國際網路安全攻防演練

為掌握我國對於突發資安事件之緊急應變能力，TWCERT/CC透過參與國際網路安全演練，以提升事件處理應變能力。以下以APCERT網路安全演練進行說明。

APCERT是亞太地區最具公信力的國際網路安全事件危機處理的協作組織，至2016年12月為止，亞太地區已有20個經濟體，共28個組織參與成為會員，台灣由TWCERT/CC及TWNCERT及EC-CERT三個單位以正式會員身分參與APCERT之運作。APCERT每年定期舉行APCERT線上資安演練，以測試亞太地區經濟體內主要網路危機處理組織的應變能力，TWCERT/CC除了與中山大學TACERT一同參與演練外，自2016年起，TWCERT/CC參與APCERT演練腳本設計，從演練主題訂定、演練角色安排、演練設備籌備至整個演練腳本完整訂定，皆由該設計團隊全盤負責。APCERT線上資安演練主題為「Emergence of a New DDoS Threat」，演練時間為2017年3月22日，腳本演練方式是模擬現實生活中的案例，以測試緊急計畫及特定弱點(抵擋大規模網路攻擊)，增加各組織間的密切合作與國際通報流程及管道。本次參與演練的成員計有日本JPCERT/CC、韓國KrCERT/CC、香港HKCERT、中國CNCERT等23個亞太地區CERT(計18個經濟體)，另外還有來自OIC-CERT的4個成員國(埃及、摩洛哥、奈及利亞和巴基斯坦)的4個CSIRT，我國參與單位計有TWCERT/CC、TWNCERT及EC-CERT。

在正式演練進行前，先進行連線及E-Mail信件寄送，以測試所有連線及收發信件正常運作，而在演練執行期間則針對APCERT負責此次線上演練團隊寄送一個事件狀況，參與演練之會員需要針對事件狀況採取相對應的應變狀況，將應變狀況以信件的方式回覆。

一、國際資安組織交流現況

(三)國際定期互訪

為了促進國際學者與TWCERT/CC交流及研討，已邀請日本Nippon CSIRT Association(NCA)學者Masato Terada(寺田真敏)前來擔任9月13日TWCERT/CC舉辦之「2017台灣資安通報應變年會」演講嘉賓，Masato Terada於會議中對於NCA協處資安事件之相關經驗進行分享，從會議中不僅可以了解日本協處事件之作法，也可彼此切磋琢磨，以增進資安事件應變時效。

11月22日也邀請日本Panasonic內部PSIRT(Product Security Incident Response Team)負責人林永熙先生，來台參與中日工程研討會，除了分享Panasonic內部PSIRT運作機制外，也針對推動企業成立CSIRT給予相關建議，以供未來TWCERT/CC在做企業內部成立CSIRT推廣時之參考。

上圖35 Masato Terada於2017台灣資安通報應變年會座談會進行分享

右圖36 TWCERT/CC主任陳永佳致贈Panasonic主幹技師林永熙禮品

一、國際資安組織交流現況

(四)國際情資交流

為擴大國際合作交流，TWCERT/CC積極加強國際資安組織交流，並與國外資安情資平台介接，掌握國際資安最新政策、情資及發展趨勢。除維持蒐整既有外部情資來源管道，2017年加入美國國土安全部之自動化威脅分享(Automated Indicator Sharing, AIS)計畫、反釣魚工作小組(Anti-Phishing Working Group, APWG)計畫、並取得我國惡意IP及釣魚網站等相關資安情資後通報我國政府、學術網路及民間單位；另加入No More Ransom專案並成為合作夥伴，取得最新勒索病毒情資，亦獲授權進行正體中文版網頁翻譯；亦加入STOP.THINK.CONNECT、2017 Cyber Security Awareness Month(NCSAM) Champion 及 2018 Data Privacy Day Champion 會員，取得資安教育及推廣素材，並翻譯成中文後供民眾閱覽、強化國內網路安全環境之維護。

除由上述管道取得情資，本中心亦適時回饋情資至國際資安組織，如國內重大駭侵事件發生時，將相關情資分享至國際資安組織，例如2017年度發生之印表機勒索事件、WannaCry 及Petya等勒索軟體事件、國內某商業銀行SWIFT系統事件等，以建立國際資安聯防效益，並達到互惠互利之長久合作關係。

2017年5月與日本電腦網路危機處理暨協調中心(Japan Computer Emergency Response Team Coordination Center，JPCERT/CC)完成合作備忘錄之續簽，效期為五年，後續雙方將持續在資安相關計畫中合作，並在各國既有法律及政策下，共同合作以對於資安事件進行應變，並增加國際聯防之能量。

二、2017台灣資安通報應變年會成果紀實

近年來台灣發生數起重大資安事件，從2016年勒索軟體案件數增長、一銀ATM盜領案、遊戲公司遭受DDoS攻擊事件，到今(2017)年初證券交易商遭DDoS攻擊勒索等事件，除了讓台灣受駭業者之業務遭受重大影響外，也反映出台灣民眾普遍資安意識不高，資安防禦措施及資安應變機制不夠完善，因此，如何強化與改善已成為當今重要議題。

台灣目前在政府、電子商務、民間、學術界、電信業者、資安公司及研究單位皆已成立CERT/CSIRT，提供資安事件通報、研析、協調應處等服務，若發生資安事件時，第一時間應尋求該領域之CERT/CSIRT相關協助，但目前台灣社會大眾對於資安事件通報並不了解，甚至不知道各個CERT/CSIRT所提供的服務內容，因此當企業遭遇資安事件時不清楚可尋求哪些單位提供相對應的協助，而使得機關與企業內部受到極大損失。

透過TWCERT/CC於2017年9月13日假北科集思會議中心舉辦2017台灣資安通報應變年會，聽眾對於資安通報應變流程、台灣現有之CERT/CSIRT所提供的服務內容、強化企業內部教育訓練辦法、資安公司協助企業處理資安事件所採取的應變措施、防護作為及相關資安產品解決方案等內容可有更進一步的了解，期許未來台灣各領域之企業在面臨資安事件時，可在第一時間找到適合的資安公司/單位來進行相關協助，並透過資安事件通報應變機制，達到資安整合聯防之目的。

此次會議從上午至下午共包含27個議程，除了邀請國內資安專家分享外，也邀請到NCA委員會主席Masato Terada來到會場為大家分享日本NCA的運作，此次研討會是TWCERT/CC自2015年國家中山科學研究院承接以來，首次舉辦的大規模的資安研討會議，當天約有330人共襄盛舉，是個盛大的資安年會。

行政院資通安全處簡宏偉處長也於會中針對「我國資安聯防機制」進行相關分享，國家資安發展關鍵指標主要由完備資安基礎環境、建構國家資安聯防體系、孕育優質資安人才及推升資安產業自主能量等四個面向來衡量，目前行政院資安處初期已成立針對金融單位的資安服務團，該團成員共有10人，並希望能在2017年成立4個資安服務團。至於資安風險評估面向，則是以早期預警、持續監控、通報應變及協助改善等四面向，來落實以風險管理為核心的資安防護，其中通報應變是最重要的部分，唯有進行資安事件通報，才能掌握目前狀況，即時應處。

二、2017台灣資安通報應變年會成果紀實

會中特別邀請到台灣CERT/CSIRT聯盟成員前來分享「各CERT/CSIRT內部運作及提供的服務內容」，目前台灣CERT/CSIRT聯盟成員包含政府部門的TWNCERT、學術網路的TACERT及TWCSIRT、電子商務的EC-CERT、通傳會的NCC-CERT、趨勢科技的TM-CSIRT及民間產業的TWCERT/CC。台灣CERT/CSIRT聯盟的目的，是希望能透過台灣的這些CERT/CSIRT密切合作，即時掌握台灣的資安狀況，並即時處理緊急資安事件。此外，台灣仍有其他CERT/CSIRT尚未加入聯盟組織，未來將持續邀請台灣各個CERT/CSIRT加入聯盟，以擴展台灣CERT/CSIRT聯盟規模，並達到全台資安聯防之目的。

除了邀請CERT/CSIRT外，也非常榮幸邀請到各大資安廠商高階主管、資安社群TDOH創辦人沈家生、HITCON常務理事長Allen、駭客書院謝副院長、調查局周科長、台灣數位鑑識發展協會林理事長、中科院資安防護組陳組長，以及台灣科技大學資訊工程系鄭教授前來為我們進行相關資安協處、人才培育及通報應變等相關分享。而在研討會會場外也有安排9個資安廠商及1個駭客社群進行資安防護做法推廣，透過研討會問卷回收並分析後，此場會議約有84%的與會人員對於此次會議的舉辦相當滿意，而在會後也有一些媒體記者，如iThome、Digitimes、軍聞社、青年日報、新新聞、警廣、中時電子報及經濟日報等媒體，為此次的研討會進行相關報導。

二、2017台灣資安通報應變年會成果紀實

圖37 貴賓合影

圖39 報到現場

圖38 貴賓簽到現場

圖40 研討會現場

二、2017台灣資安通報應變年會成果紀實

圖41 研討會現場

圖42 研討會現場

圖43 貴賓致詞

圖44 餐點布置

結語

隨著科技的進步，現今已走入IoT的世代，任何物品都可連上網路，為此也產生了許多網路安全問題，從個人、企業到國家，也漸漸對於網路安全擁有相當大的危機意識，許多人為了因應網際網路威脅逐年攀升的狀態，開始著手於資安防護，不論是買防毒軟體、建構防火牆，或大手筆購入資安威脅偵測系統等等，希望透過這些資訊產品來加強資安的防護能量，以減低駭客入侵的損失，但仍有許民眾了解資安的重要性，想要將資安做好，但是不知從何著手，對於資安防護沒有基礎的概念，或者用不適當的方式來進行，這樣一來不僅花了大筆的資金，但卻沒有達到應有的效益，這時若有一位資安顧問協助，應該就能解決這些問題，目前除了可找資安公司協助外，另外的做法就是找CERT/CSIRT進行相關資安諮詢。

對於民間個人、企業組織及產業公協會等皆為TWCERT/CC的服務對象，除了提供資安諮詢的服務外，最重要的就是協助進行資安通報及處理，現今的資安防護型態已不再是單打獨鬥的模式，透過通報作業及去識別化情資互享的方式，不僅可對於資安態勢有更進一步了解外，對於個人或企業的潛在資安威脅，也可提早防範，減低資訊安全事件所造成的損失，因此資安聯防已是現今資安防護之最新趨勢。

結語

從2017年資安通報的狀況來看，以下將整理出對於個人及企業較需注意的10項資安威脅防護建議：

1. 個資外洩

- 個人：不輕易將個人資料留於網路上。
- 企業：對客戶資料善盡保護責任，否則可能會因違反個資法而遭求償，或商譽受損。

2. 社交工程攻擊

- 開啟郵件及附檔時需小心謹慎，勿開啟不明來源信件，安裝防毒軟體。

3. 勒索軟體攻擊

- 開啟不明來源信件，系統定期更新、資料需備份，安裝防毒軟體。

4. 網站/系統弱點攻擊

- 系統開發納入源碼檢測、弱點掃描及滲透測試等安全軟體發展流程(Secure Software Development Life Cycle, SSDLC)，並進行系統定期更新。

5. 釣魚網頁

- 勿點擊不明網頁連結，安裝防毒軟體。

6. 弱密碼

- 修改預設密碼，定期更新密碼，注意密碼複雜性。

7. 機密資料外洩

- 資料加密，勿將資料隨意置於雲端或上傳國外程式分析平台。

8. Webcam、印表機(事務機) I oT遭控制利用

- 勿使用預設帳密，非必要勿暴露於網路中。

9. APP偽冒

- 開發商：上線前需進行安全檢測。
- 用戶：勿安裝不明來源App。

10. DDoS攻擊

- 用戶：弱點與惡意程式檢測，並安裝防毒軟體，以避免成為DDoS攻擊幫兇。
- 企業：建置DDoS防護機制。

聯絡TWCERT/CC

- 免付費服務電話：0800-885-066
- E-mail：twcert@cert.org.tw
- TWCERT/CC官網：https://twcert.org.tw
- TWCERT/CC Facebook粉絲專頁：https://www.facebook.com/twcertcc/
- TWCERT/CC免費資安電子報訂閱：https://goo.gl/forms/MC9RH3a9qJNJ3R7x1

TWCERT/CC FB粉絲專頁

TWCERT/CC官網

TWCERT/CC資安電子報

參考資料

[01]趨勢科技。 "變臉詐騙案件猖獗,全球損失金額兩年飆長13倍", Retrieved December 11, 2017, from the World Wide Web: https://blog.trendmicro.com.tw/?p=18547

[02]ICO. (2014, November 20). “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！”, Retrieved December 13, 2017, from the World Wide Web: https://www.ithome.com.tw/news/92459

[03]SucuriSecurity. (2016, June 27). "Large CCTV botnet leveraged in DDoS attacks", Retrieved February 15, 2017, from the World Wide Web: https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html

[04]Ionut Arghire. (2016, October 28). "Mirai botnet infects devices in 164 countries", Retrieved February 15, 2017, from the World Wide Web: http://www.securityweek.com/mirai-botnet-infects-devices-164-countries

[05]Milena Dimitrova. (2016, June 28). "CCTV botnet performing layer 7 DDoS attacks global businesses", Retrieved February 15, 2017, from the World Wide Web: http://sensorstechforum.com/cctv-botnet-layer7-ddos-attacks-global-businesses/

[06]Kerneron Security. (2016, March 22). "Remote code execution in CCTV-DVR affecting over 70 different vendors", Retrieved February 15, 2017, from the World Wide Web: http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html

註：點擊參考資料頁之引用編號可返回原文頁。

參考資料

[07]US-CERT. (2016, October 14). "Heightened DDoS threat posed by Mirai and other botnets", Retrieved February 15, 2017, from the World Wide Web: https://www.us-cert.gov/ncas/alerts/TA16-288A

[08]Technews. (2017, May 13). "勒索軟體WanaCrypt0r 2.0攻擊全球Windows系統漏洞，台灣、中國也遭殃", Retrieved May 13, 2017, from the World Wide Web: http://technews.tw/2017/05/13/ransomeware-wanacrypt0r-2/

[09]TWCERT/CC. (2017, May 16). "WanaCrypt0r (WanaCry)勒索軟體行為分析報告", Retrieved May 16, 2017, from the World Wide Web: https://twcert-official-file.s3.hicloud.net.tw/TWCERTCC-MIFR-2017001.pdf

[10]Vixual. (2013, May 30). “用 Fail2Ban 防範暴力破解 (SSH、vsftp、dovecot、sendmail)”, Retrieved July 14, 2017, from the World Wide Web: http://www.vixual.net/blog/archives/252

[11]Ionut Arghire. (2016, October 28). "Mirai botnet infects devices in 164 countries", Retrieved February 15, 2017, from the World Wide Web: http://www.securityweek.com/mirai-botnet-infects-devices-164-countries

[12]Milena Dimitrova. (2016, June 28). "CCTV botnet performing layer 7 DDoS attacks global businesses", Retrieved February 15, 2017, from the World Wide Web: http://sensorstechforum.com/cctv-botnet-layer7-ddos-attacks-global-businesses/

註：點擊參考資料頁之引用編號可返回原文頁。

參考資料

[13]聯合新聞網。 “後門被攻破 金管會指遠銀資安不嚴謹 疑有人為疏失”, Retrieved October 07, 2017, from the World Wide Web: https://udn.com/news/story/7239/2745552

[14]自由時報。 “金管會：遠銀有漏洞 駭客入侵「走後門」”, Retrieved October 08, 2017, from the World Wide Web: http://news.ltn.com.tw/news/focus/paper/1141809

[15]金管會。 “金管會對遠東銀行發生電腦駭客事件說明”, Retrieved October 06, 2017, from the World Wide Web: https://www.fsc.gov.tw

註：點擊參考資料頁之引用編號可返回原文頁。