資訊安全

針對勒索病毒網路風險管理與資訊安全防護技術研究

空軍備役上校　吳嘉龍

提要

當前駭客攻擊手法也隨科技發展日新月異，伴勒索病毒(勒索軟體/綁架病毒)惡意程式攻擊型態迅速竄起，造成政府部會、單位組織及個人頻遭網路駭客侵擾或竊密之資安事件日增，嚴重影響資訊作業安全，因此，本文將針對勒索病毒網路風險管理與資訊安全防護技術深入探討。值得注意的是，趨勢科技在2016年上半年就發現了79個新的勒索病毒家族，這數字相較2015年整年的數量增加179%；2016年勒索病毒新家族數量更成長了752%。事實上，駭客除不斷創新和更新犯罪工具之外，包括運用DDoS(分散式阻斷服務攻擊)、零時差攻擊、網路釣魚與變臉詐騙攻擊等惡意程式攻擊手法，更不斷從現有的目標當中積極找尋更多潛在受害者，同時也採用社交工程等攻擊來提高獲利。根據趨勢科技Trend Labs報告發現，高達99% 的勒索病毒都是透過電子郵件或網站連結進行散播攻擊，案例更顯示，感染勒索病毒Ransomware受害者當中，近30%是重複感染，肇因分析是未即時修補伺服器安全漏洞形成防護空窗，因此讓惡意程式攻擊有機可乘，定期修補系統並且防堵漏洞，仍是防範零時差漏洞與潛在攻擊的最佳方式。

關鍵字：勒索病毒、緊急應變、資訊管理、網路安全、惡意程式。

壹、前言

近年網路安全及資料外洩等問題，一直困擾政府機關及民間企業，其中駭客入侵、病毒感染及惡意程式肆虐等事件層出不窮，因而造成網路中斷、重要資料被竊等情事時有所聞。趨勢科技全球技術支援與研發中心研究分析，2016年重大網路資安事件層出不窮，2016年是大型資料外洩頻傳的一年，就受害者數量來說，Yahoo大量用戶帳號密碼被駭應該是最大的一宗案例。勒索病毒開放原始碼出現及勒索病毒服務(Ransomware as a Service，簡稱RaaS)讓網路犯罪集團輕易發動勒索病毒攻擊，企業最新的惡意程式攻擊威脅包括新的勒索病毒家族數量成長752%、平均每起變臉詐騙讓企業損失約14萬美金，由於許多使用者習慣在不同的網站上重複使用相同的使用者名稱以及密碼，因此這些帳號也因而立即陷入危險[1]。回顧2015年4月到2016年4月的行動勒索病毒Ransomware(勒索軟體/綁架病毒)時，趨勢科技研究注意到Android勒索病毒數量的大幅上升。在這段時間內，Android勒索病毒數量增加了140%。在某些區域行動勒索病毒甚至佔行動惡意軟體總數的22%，其中分散式阻斷服務(DDoS)惡意程式攻擊是最受關注的焦點，因為2016年出現了多起大型攻擊案例，關鍵是運用Mirai木馬程式作為攻擊工具，受Mirai感染的裝置會持續地在網際網路上掃描物聯網裝置的IP位址，因此許多物聯網(Internet of Thing，簡稱IoT)裝置都有可能成為受害者。Mirai惡意軟體可以使執行Linux的計算系統成為被遠端操控的「殭屍」，以達到通過殭屍網路進行大規模網路攻擊的目的。Mirai殭屍網路大約掌控了全球10萬個物聯網裝置，在掃描到IP位址之後，Mirai會通過超過60種常用預設使用者名稱和密碼辨別出易受攻擊的裝置，然後登入這些裝置並植入Mirai軟體。若感染Microsoft SQL及MySQL等資料庫，Mirai程式就會建立具有管理員權限的使用者帳號，便可能執行多種惡意任務，包括啟動執行檔、刪除檔案、植入自動啟動的圖示或在Windows registry建立相應log檔，可為駭客開啟後續攻擊或竊密資料的大門。分散式阻斷服務(DDoS)攻擊，造成資安部落格KrebsOnSecurity停擺的Mirai木馬程式本來只鎖定Linux裝置，現在已經演化出能感染Windows裝置的版本，擴大原始Mirai的感染範圍。網路使用者應隨時保持警戒才能避免損失資料與金錢，同時避免大規模停機可能性；採用多層式防護，包括閘道防護、端點防護、網路防護、伺服器防護，將可有效防範勒索病毒惡意程式攻擊感染[2]。

貳、勒索病毒惡意程式攻擊網路安全威脅分析

在2016年惡意程式攻擊威脅情勢屢創新高，包括新的勒索病毒Ransomware(勒

索軟體/綁架病毒)家族掘起、發現全球肆虐變臉詐騙以及各種平台軟體漏洞頻傳，依據趨勢科技研究，「2016年資訊安全總評：企業威脅刷新紀錄的一年」的報告指出去年威脅包括有：勒索病毒大幅成長(據統計分析，勒索病毒家族數量從原本的29個增加到247個)、變臉詐騙日益猖獗(變臉詐騙就運用社交程式攻擊為網路犯罪集團帶來龐大獲利，全球企業平均案例損失金額高達14萬美元)、軟體漏洞層出不窮(趨勢科技和Zero Day Initiative所發掘的漏洞數量在2016年創下新高，其中發現最多的是Adobe Acrobat Reader DC的漏洞)、銀行木馬程式和ATM惡意程式(網路犯罪集團會利用ATM惡意程式、盜拷磁條以及銀行木馬程式來從事犯罪)、Mirai木馬程式讓殭屍電腦發動大規模攻擊(2016年10月，物聯網(IoT)裝置遭到駭客入侵並用於發動分散式阻斷服務攻擊，約有10萬台物聯網裝置遭到入侵，並且導致Twitter、Reddit、Spotify、Flickr等知名網站斷線數個小時)、以及Yahoo發生史上最大宗資料外洩(2013年8月Yahoo發生了有史以來最大一宗資料外洩，高達10億個帳號的使用者資料遭到外洩；2016年9月Yahoo再次發生另一起資料外洩，又有5億個帳號受害)。趨勢科技「資安攻防新層次-趨勢科技2017年資安預測」報告指出，勒索病毒會開始朝不同方向發展，行動勒索病毒迅速發展，2017年資訊安全威脅預測整理如表一[3-4]。

勒索軟體常偽裝成假防毒軟體安裝程式，並利用人性弱點運用社交工程(social engineering)技巧來誘騙或恐嚇使用者點選其連結或詐取使用者的帳號密碼，使用者可能因為開啟了惡意電子郵件或網站上的檔案而不小心下載並安裝了勒索程式。勒索病毒的迅速擴張發展預料會刺激網路犯罪，進而發展多樣化及擴展相關惡意攻擊平台、能力和技術，讓惡意程式攻擊者發掘更多的目標。趨勢科技全球技術支援與研發中心報導2013年出現了一種加密勒贖程式(Crypto-Ransomware)新型態勒索程式，CryptoLocker就是其中之一，該程式不僅會鎖住受害者的電腦，還會將其檔案加密，如此可以確保即使惡意程式遭到清除，受害者也可能會為了解開檔案而支付贖金。一般的網路釣魚(Phishing)和魚叉式網路釣魚(Spear Phishing)所使用的技巧類似，明顯差異在於網路釣魚基本上是一種針對大量目標的亂槍打鳥式攻擊，但魚叉式網路釣魚則是專門針對特定目標。一般的網路釣魚攻擊目的在偷取受害人的資料，但魚叉式網路釣魚攻擊來說，取得登入資訊或個人資訊通常只是攻擊開端，這是攻擊進入目標網路手段，等於是作為針對性攻擊/鎖定目標攻擊(Targeted attack)跳板。目標式社交工程攻擊(Spear-Phishing & Social Engineering Malicious Attack)是利用網路為媒介或工具，針對特定目標人士所進行之詐騙手法，它避開較不容易破解的網路防火牆，攻擊人性弱點，是非常難以防範的攻擊模式。儘

表一、2017年資訊安全威脅預測分析表(自行整理)

項目	資安攻防新層次-趨勢科技 2017 年資安預測
勒索病毒成長力道將開始平緩，但攻擊手法將朝多元化發展	勒索病毒高峰期在2016年發生，進入穩定期後，駭客惡意程式攻擊朝著多元化發展，讓勒索病毒蔓延至更多潛在受害者、找尋平台及更大型的攻擊目標。非桌上型電腦終端機(包括ATM提款機、PoS銷售櫃台系統與手機和平板等行動裝置)同樣遭到勒索病毒攻擊
物聯網僵屍病毒將進行分散式阻斷服務攻擊，物聯網系統將成為針對性攻擊的目標	運用物聯網IoT裝置的殭屍網路若發動流量放大技巧可以進行DDoS攻擊，並且將造成更大傷害。2017年起，包括一些服務導向、新聞電子媒體、影音平台、企業和政治相關的網站，將遭到有系統的大規模HTTP流量攻擊，製造這些智慧型裝置及設備廠商，應於產品開發過程中將資訊安全列為重點主動降低風險。使用者也必須預先設想歹徒可能的攻擊情境，藉此找出並防範可能出問題的環節
變臉詐騙容易得逞、經濟效益極高，且不需太多基礎架構，將使針對性詐騙數量增加	假冒求職信，偽裝履歷表PDF檔案與暗藏惡意巨集Excel試算表，覆寫系統硬碟主要開機磁區；分析以全球企業財務部門為攻擊目標「變臉詐騙」，其手法是先駭入某個電子郵件帳號，然後再透過該帳戶指使員工將一筆款項匯到歹徒的銀行帳戶。變臉詐騙郵件特別不容易偵測，因為這類郵件並未挾帶惡意程式或執行檔，不過企業仍可利用網站閘道或電子郵件閘道端的防護產品來攔截這類威脅
商業流程入侵逐漸獲得網路犯罪集團重視，目標鎖定財務相關部門	有別於變臉詐騙利用的是人為疏失，網路搶劫若針對大型機構處理金融交易的流程下手，我們將這類攻擊稱為「商業流程入侵」(Business Process Compromise，簡稱BPC)。網路犯罪集團發動BPC首要攻擊目標是為了錢，而非為了政治動機或蒐集情報，然而這些攻擊和鎖定目標攻擊所採用的方法和策略非常類似。BPC的攻擊對象並不只侷限於財務部門。其可能的攻擊手法包括：駭入採購系統，進而暗中攔截原本應該匯給廠商的款項。此外，駭入付款流程系統也能收到類似效果。另一種手法是駭入出貨中心的電腦系統，將高價值的商品轉寄至歹徒指定地點，造成企業組織相當大的損失
Adobe和Apple平台新發現軟體漏洞數量將超越Microsoft	根據資安風險分析，除Microsoft之外，未來Adobe和Apple的產品也將發現更多的軟體漏洞；除了因為Windows PC出貨量近年來持續衰退之外，另一項因素是有越來越多使用者平常使用智慧型手機或商用平板而非一般電腦。當購買Mac電腦消費者越來越多，歹徒的目光就會開始轉向Apple的軟體漏洞，漏洞防堵技術是有效主動防範未修補漏洞和零時差漏洞的方法，Apple和Adobe使用者也應妥善保護自己的端點和行動裝置，以防範這類惡意程式攻擊
惡意程式攻擊者將開發出躲避偵測技術開發最新針對性攻擊手法	駭客為了逃避偵測工具的檢查，過去駭客大多使用執行檔，後來改用文件檔案，而現在則是較常使用腳本和批次檔。他們將開始運用一些更複雜的沙盒偵測技巧，並且觀察目標網路是否會將未知檔案傳送至沙盒模擬環境當中分析，甚至會攻擊沙盒環境，讓沙盒模擬分析失去作用。此外，虛擬機器規避(VM Escape)的技巧將成為進階漏洞攻擊程序當中備受重視的元素。虛擬機器跳脫技巧除了能夠躲避沙盒模擬分析之外，在雲端當中也有各種不同的攻擊應用發展

管勒索病毒攻擊並無百分之百有效的預防措施，然而，最好的方法還是藉由網站與電子郵件閘道防護，從來源攔截這類威脅，目標式社交工程攻擊與駭客攻擊伎倆分

析表整理如下列表二[5-6]。

表二、目標式社交工程攻擊與駭客攻擊伎倆分析表(自行整理)

項目	目標式社交工程攻擊與駭客攻擊伎倆
電子郵件標題誤導夾藏陷阱	社交工程(social engineering)攻擊運用電子郵件標題如下：退稅通知/求職信/電子訃聞、電子帳單/電子發票、iPhone中獎通知、Google Chrome和Facebook重大更新和通知訊息、訂單確認/付款收據、文件請求/審計報告/預算報告、誘騙使用者連到假冒真正銀行或政府機構網站的網頁連結、輸入驗證碼以及帳戶欠款已過期/無法派送貨物等等，令人防不勝防
亂槍打鳥網路釣魚	網路釣魚(Phishing)企圖透過電子郵件、通訊軟體來獲得個人資訊以竊取使用者身份認證。大多數網路釣魚手法會企圖讓外表看來像是一般行為，實際上卻是用於犯罪活動，例如藉由電子郵件、網頁掛馬或Web2.0應用，吸引使用者接連結惡意網頁，或製作假網頁，誘騙使用者輸入帳號、密碼或信用卡等資料或不知情狀況下載執行惡意程式而遭受攻擊
標籤綁架網路釣魚	標籤綁架(Tab-napping)網路釣魚手法藉由使用者造訪駭客特製內含惡意程式的網頁，相關惡意程式便可偵測此使用者經常使用或正在使用的網路應用服務(網頁)，在使用者點選其它網頁而暫時離開惡意網頁時，惡意網頁會改變其顯示內容，變身為使用者經常或正在使用的網路應用服務，以誘騙使用者輸入帳號密碼。此攻擊手法比起傳統釣魚郵件或社交網站惡意連結手法，大幅簡化網釣攻擊程序，且更容易讓使用者上當受騙，意謂此攻擊將比傳統網釣手法運作更具殺傷力，且影響層面廣泛。
魚叉式網路釣魚	魚叉式網路釣魚(Spear Phishing)是專門針對特定對象的網路釣魚，其對象通常是某個機構，通常鎖定特定個人或某機構的特定員工及其社群媒體帳號(如Twitter、Facebook和LinkedIn)，目標是取得機密資訊，技巧包括假冒他人名義、使用誘餌、避開安全機制。此手法也是造成JP Morgan、Home Depot、Target以及醫療保險Anthem Inc.大規模資料外洩主因，此攻擊常會鎖定特定個人或某機構特定員工及其社群媒體帳號，誘騙目標對象開啟郵件附件檔案或點選連結，當開啟檔案或連結，將執行惡意程式或將使用者導向某個網站，駭客建立其祕密通訊網路
即時通及社交網站	透過即時通軟體(Windows Live Messenger、Yahoo Messenger、LINE、WeChat、Skype、Google Talk等)或社交網站(Flickr、Qzone、Instagram、LinkedIn、Facebook、Twitter、Plurk、Google+等)，偽冒或盜用受害人身分，主動傳送惡意程式、超連結給社交群組連絡人，或進行請求代購遊戲點數、代為使用ibon、FamiPort及Life-ET等超商便利站代收機、ATM轉帳等各項詐騙，遭植木馬程式與病毒擴散、個資外洩或財物損失
針對性攻擊/鎖定目標攻擊	針對性攻擊/鎖定目標攻擊(Targeted attack)手法分析，駭客會利用各種最新時事、業務相關內容，以及攻擊目標可能有興趣的資訊來從事社交工程攻擊。值得注意的是，後門程式、零時差或軟體漏洞攻擊、水坑式攻擊、魚叉式網路釣魚等等，也是歹徒經常用來竊取資訊的技巧，此種攻擊重點在於必須根據受害者的防禦機制而調整及改進其攻擊方法
網站/網頁式攻擊	網站(頁)式攻擊(Web-based Attack)，駭客攻擊之目的從求名轉變為求利，其手法也隨之轉變由以往置換網頁(Defacement)的攻擊模式改為掛馬(Embeded)的攻擊模式；且伴隨Web 2.0應用興起，上網瀏覽從靜態網頁，轉變為可編輯網頁內容的互動式網頁。因此，攻擊網站(頁)應用程式，插入惡意連結或程式碼，致使用者瀏覽該網頁受駭或竊取個資(Drive-by download Attack)，儼然成為駭客攻擊新興社交工程手法

參、勒索病毒理論技術與趨勢發展分析

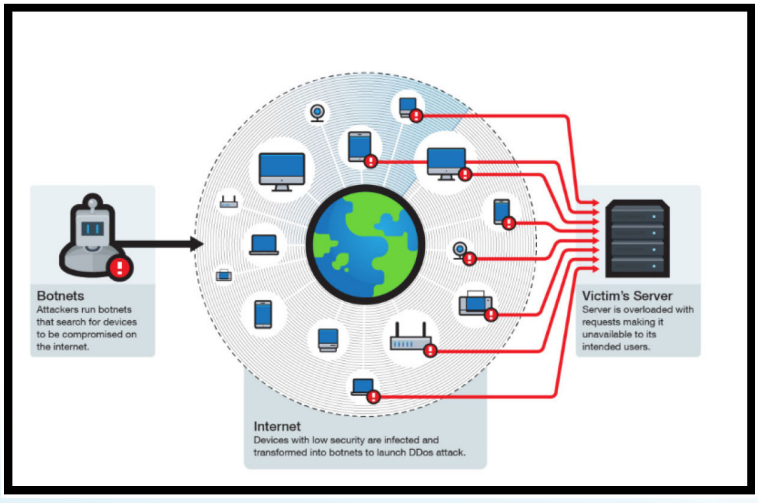
TREND LABS趨勢科技全球技術支援與研發中心研究指出，2016年上半年觀察到網路犯罪分子利用像JavaScript、VBScript和Office巨集文件等檔案類型來躲避傳統的安全解決方案。有些可以直接用來編寫惡意軟體。Unwire Pro調查結果顯示，近日網路安全公司Fortinet公布數據指，勒索軟體Cerber的散布率正急速上升，與CryptoWall和Locky成為前3名廣泛散布的勒索軟體威脅。網路安全公司Fortinet透過其FortiGuard Intrusion Prevention System(IPS)內200萬個安全節點收集數據，發現2016年4月1日至5月15日期間，Cerber的散布率正急速上升，貼近首兩位的CryptoWall及Locky，成為2016年勒索軟體中的第三大威脅。像Locky和Cerber這些常見的勒索病毒也是使用一般的社交工程主旨。最新的Locky變種會使用DLL和.HTA檔案類型來散播。Locky使用VBScript附件檔，容易進行混淆來躲避偵測。Locky垃圾郵件可能使用其他可執行檔如.COM、.BIN和.CPL來散播病毒威脅，因此須封鎖夾帶有JS、VBScript、WSF和HTA附件檔的垃圾郵件，具備黑名單機制的解決方案可以封鎖已知的惡意發送IP地址。要偵測Locky和Cerber巨集下載程式，電子郵件解決方案應具備巨集掃描功能，能夠偵測病毒威脅惡意巨集元件，由於電子郵件是針對性攻擊入侵企業最普遍的管道，加密勒索軟體(勒索病毒/綁架病毒)最大宗的攻擊方式是透過網路釣魚信件，只要開啟陌生人寄來的信件即可能受到病毒攻擊因此，防範魚叉式網路釣魚攻擊是一項非常重要的工作。而要防範網路釣魚，針對於員工的教育訓練相形重要；包括訓練員工觀察郵件內的拼字錯誤、奇怪用詞，以及其他可疑的徵兆，就能有效預防一定程度的魚叉式網路釣魚。除此之外，積極作為需要

表三、防範勒索病毒行為(自行整理)

項目	綁架/勒索病毒攻擊伎倆分析
打字太快誤按到鍵	加密勒索軟體最大宗的攻擊方式是透過網路釣魚信件，如打字或不小心按到其他鍵，當心誤點進入到網路釣魚網站而遭受攻擊
假冒銀行網路釣魚	利用使用者對往來銀行的信任，病毒電郵偽裝成銀行發出的電郵，誘使收件人開啟，或者製作網路釣魚頁面來獲取使用者金融和相關個人資訊
誤信搜尋引擎結果	網路詐騙集團或駭客針對使用搜尋引擎新聞習慣，採用搜索引擎禁止的暗黑作弊手法優化網站，被害的網友點擊相關新聞時被事前埋伏惡意網頁攻擊
假冒執法警告信函	自稱網路警察或執法機構詐騙集團謊稱因觸犯法規電腦遭鎖定，須支付罰款才能解除鎖定，實際上是勒索病毒慣用的攻擊手法
勒索病毒社交工程	大型企業和中小型企業都應該要留意郵件主旨，像是發票、包裹快遞、訂單確認、銀行通知和付款收據等，有效來察覺勒索病毒所用電子郵件
偽冒盜用數位簽章	假藉、偽冒或盜用軟、硬體或防毒軟體公司之數位簽章，致惡意程式可躲避防毒軟體偵測，並降低使用者之戒心，誘騙使用者執行

建立更完整的多層次防護，來讓系統管理員確切掌握及掌控網路的狀況，進而降低針對性攻擊的資安風險，防範各種攻擊途徑，以下針對勒索病毒攻擊行為整理分析如表三[7-8]。

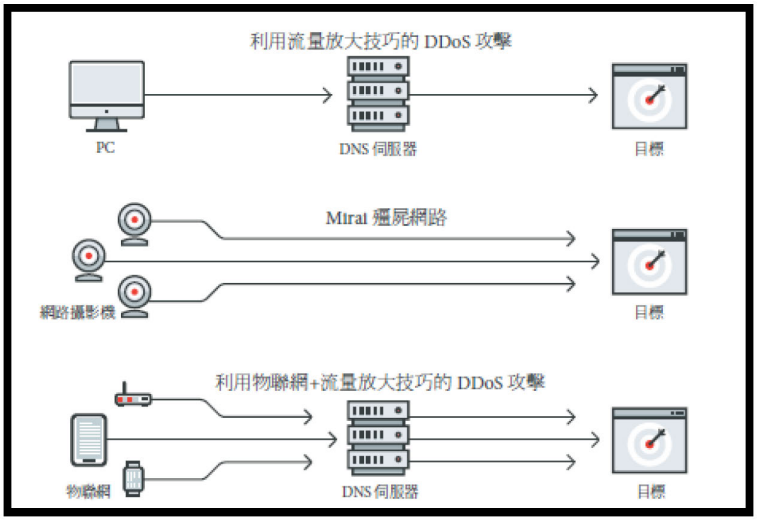
勒索病毒家族數量去年飆升7倍，趨勢科技統計，受勒索病毒攻擊次數全球排行榜中，台灣排名第18名，仍屬於資安高風險國家，亞洲中更是僅次於印度、越南、印尼、日本、菲律賓、泰國等國，亞洲排第7。駭客善於利用竊來的帳號資料來進行所謂的網路釣魚攻擊，偽裝成Gmail、Yahoo或其他公司來寄送電子郵件給目標。從資訊安全的角度來看，工業與環境控制設備無身份驗證機制或使用預設密碼，並曝露於網際網路上，恐有資訊外洩與遭受入侵之疑慮，事實上，物聯網(IoT，Internet of Thing)裝置存在著一些基礎的弱點，在Mirai殭屍病毒原始程式碼在2016年公開流傳後，沒多久就被駭客用來刺探各種智慧家庭裝置，並且以預設的帳號密碼登入這些裝置，使得成千上萬的智慧裝置淪為殭屍網路的成員，幫助駭客發動多起史上最大規模的分散式阻斷服務攻擊(DDoS)攻擊。Mirai殭屍網路大約掌控了全球10萬個裝置，2016年10月Mirai勒索病毒並且對網路服務供應商Dyn服務廠商的伺服器發動了大規模DDoS攻擊，數以千計IoT遭到殭屍化的監視攝影機發動攻擊，導致許多知名網站(包括Twitter、Reddit、Spotify、SoundCloud、CNN、Airbnb、Spotify、Netflix、HBO等)因而無法使用，經研究預測網路犯罪集團將繼續利用網路攝影機與DVR數位錄影機消費型裝置的安全漏洞來建立殭屍網路以發動DDoS攻擊，案例包括在2015年12月及2016年烏克蘭電廠遭到相當精密的駭客攻擊，導致嚴重的電力中斷，未來預測將以BlackEnergy惡意程式為基礎，開發出更具威力攻擊。由於監控與資料擷取(SCADA)系統被發現的漏洞數量大幅增加，因此2017年，工業物聯網發展趨勢將為企業帶來前所未有的資安危機和風險[6-10]，圖一為Mirai勒索病毒運用殭屍網路進行分散式阻斷服務攻擊示意圖[6]，圖二為Mirai殭屍網路惡意程式發動分散式阻斷服務



圖一、Mirai勒索病毒運用殭屍網路進行分散式阻斷服務攻擊示意圖[6]

攻擊示意圖[7]。

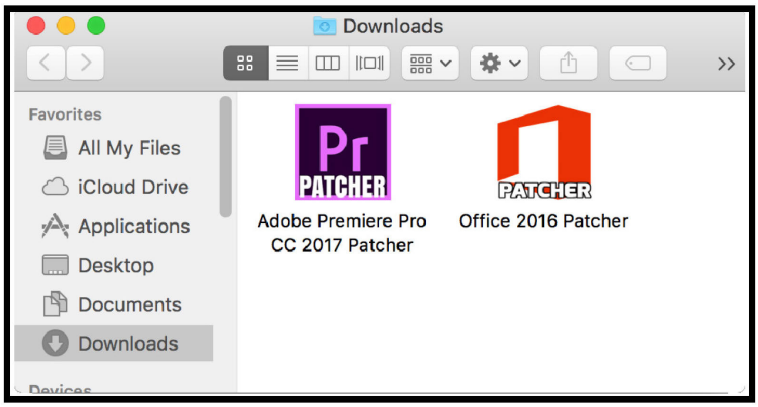
Lord Alfred Remorin(2016)研究分析指出，美國聯邦調查局(FBI)將商務電子郵件詐騙定義成針對與外國供應商合作企業或經常進行匯款支付企業的精密騙局，圖三為勒索病毒假冒美國聯邦調查局發出警告信函進行網路釣魚示意圖。根據美國聯邦調查局指出，在2013年10月到2015年8月間，商務電子郵件詐騙已經造成美國受害者將近7.5億美元的損失，影響超過7,000人。全球網路犯罪份子從美國以外的受害者詐騙了超過5,000萬美元。此詐騙手法往往從攻擊者入侵企業高階主管郵件帳號或任何公開郵件帳號開始，通常經由鍵盤側錄惡意軟體或網路釣魚方式達成。行動裝置勒索病毒在2016年大爆發，光我們2016年第四季所蒐集分析的樣本數量就是2015年同期的三倍。但儘管數量驚人，這些惡意程式的犯罪模式卻大同小異：濫用、誘騙、恐嚇、勒索。其中大部分都是濫用Android作業系統功能的螢幕鎖定程式，以及運用社交工程惡意攻擊手法偽冒系統更新、偽冒熱門遊戲與色情內容。這些程式會誘騙不知情使用者提供系統權限，進而修改裝置鎖定畫面的密碼，讓使用者無法將它解除安裝。Patcher正是一個針對MacOS作業系統勒索病毒Ransomware，首先經由bittorrent檔案下載散布，並且偽裝成Microsoft Office和Adobe Premiere Pro軟體的修補程式。Patcher勒索病毒



圖二、Mirai殭屍網路惡意程式發動分散式阻斷服務攻擊示意圖[7]

圖三、勒索病毒假冒美國聯邦調查局進行網路釣魚示意圖[9]

一旦執行，就會開始使用隨機產生的25字元加密金鑰來將檔案加密。它會將「/Users」目錄及掛載到「/Volumes」目錄下的磁碟和外接裝置所有檔案加密，圖四為Patcher勒索病毒Ransomware攻擊示意圖[9-10]。

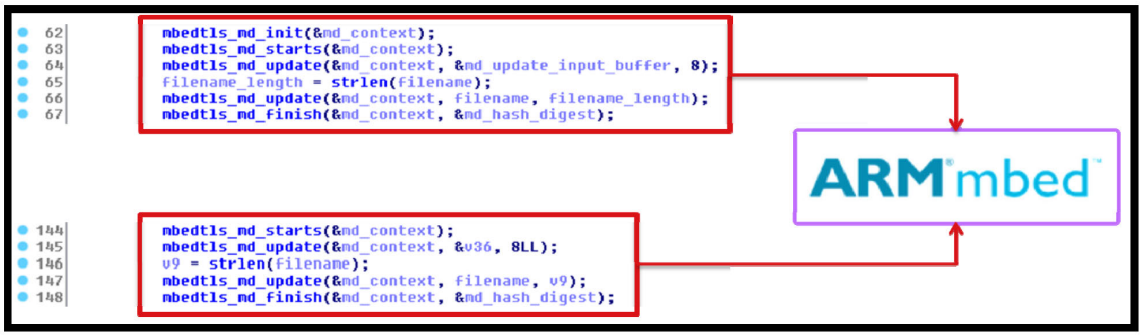


圖四、Patcher勒索病毒Ransomware攻擊示意圖[10]

根據TREND LABS研究分析，行動勒索病毒歸納如表四，行動裝置銀行木馬程式絕大多數都出現在俄羅斯，事實上，這占了我們全球偵測數量的74%。其他受害較嚴重的國家還有：中國、澳洲、日本、羅馬尼亞、德國、烏克蘭及台灣。研究指出SMSLocker是現今Android勒索病毒的開端，2016年最受矚目的Svpeng(銀行木馬程式與勒索病毒的合體)，在所發現的銀行木馬感染與攻擊案例當中，約有67%都是Svpeng惡意程式攻擊。Svpeng最起先是銀行木馬程式，之後演變成行動勒索病毒，取得加密類別後，該樣本會找出SD卡上所有檔案並加以加密。另一個是勒索病毒家族FakeToken，該惡意程式於去年發現，在成功潛入裝置

表四、行動勒索病毒攻擊歸納分析(自行整理)

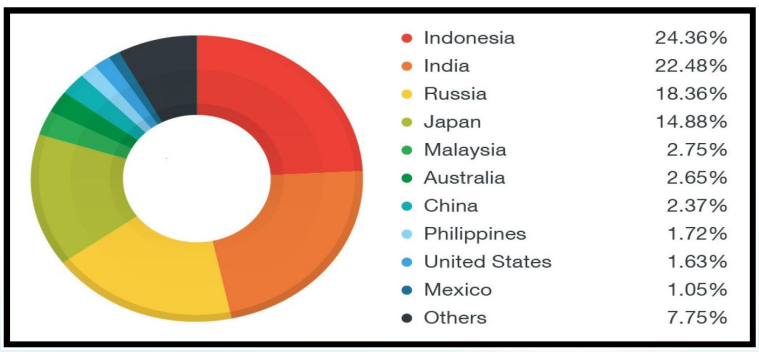
項目	行動綁架勒索病毒攻擊方式
SMSLocker (ANDROIDOS_SMSLOCKER	SMSLocker利用簡訊進行命令和控制(C&C)通訊；SLocker行動勒索病毒使用Android UI API鎖住設備螢幕
Svpeng (ANDROIDOS_SVPENG)	Svpeng主要以俄羅斯銀行為目標，受害最深的自然是俄文的使用者，尤以俄羅斯、烏克蘭和羅馬尼亞最為嚴重
FLocker/Frantic Locker (ANDROIDOS_FLOCKER)	FLocker在2016年第一季末首度現身，跨界感染智慧型電視，所偵測到FLocker樣本數量超過32,000個以上
SLocker/Simple Locker (ANDROIDOS_SLOCKER)	SLocker在顯示贖金消息時禁用“後退”按鈕以阻止用戶嘗試恢復設備正常使用，2016年印尼出現SLocker變種病毒(AndroidOS_Slocker.AXBDA)，出現大量假視訊播放程式
Koler (ANDROIDOS_KOLER)	SLocker和Koler會假冒司法機關，宣稱受害者觸犯了某種法律，藉此勒索使用者支付一筆贖金以逃避相關刑責
ZergHelper (IOS_ZERGHELPER.A)	在中國的第三方市集應用程式商店以及越南HiStore會散布含有越權廣告應用程式(IOS_LANDMINE.A)並濫用iOS執行程序功能並利用漏洞來避開 iOS隱私權保護機制
SMSSecurity (ANDROIDOS_FAKEBANK)	SMSSecurity(ANDROIDOS_FAKEBANK)這個以奧地利、匈牙利、羅馬尼亞、瑞士的銀行為主要目標的銀行木馬惡意程式，利用 TeamViewer 軟體來遙控裝置進行攻擊



圖五、惡意軟體利用Linux.Encoder和KeRanger加密程式庫示意圖[13]

後會自我隱藏，並且藉由幕後操縱通訊來破解雙重認證機制。而在Mac OS X系統上則有KeRanger，出現在被竄改過的檔案分享應用程式和惡意Mach-O檔案中，偽裝成RTF格式文件。Linux.Encoder和KeRanger加密程式庫的相似性在於都使用ARM mbed TLS，其共同點是使用Unix多使用者、帶有命令行的作業系統，具備統一的檔案系統和簡單而強大的工具，如shell和命令列語言，可以用來進行複雜的任務，它提供應用程式SSL/TLS和加密能力，圖五為Linux.Encoder和KeRanger加密程式庫示意圖[11-14]。

在此，針對勒索病毒發展最新趨勢與手法分析說明，網路攻擊利用Predator Pain和Limitless這兩個鍵盤側錄程式來從事變臉詐騙攻擊或稱為商務電子郵件入侵(Business Email Compromise，簡稱BEC)，獲利高達約22億新台幣。在研究過程，Limitless和其他工具一起被廣泛地用在針對性攻擊/鎖定目標攻擊(Targeted attack)活動。受害最深的國家是印尼、印度、蘇俄、日本、馬來西亞以及澳洲。大型跨國企業是變臉詐騙(BEC)的主要攻擊目標，這類網路詐騙通常會先入侵目標機構的某個電子郵件帳號，然後再利用該帳號來發信給該公司的財務部門，誘騙他們匯款至歹徒的銀行帳戶。受害者通常是有跟國外供應商往來、並且習慣使用電匯方式付款的企業。變臉詐騙的受害者數量從2015年初至今已成長270%，2016年更一舉突破單一企業受害金額紀錄。雖然Android作業系統機制已經可防止第三方應用程式完全掌控裝置的資料，但Android 7.0的推出，將進一步讓某些行動勒索病毒經



圖六、TREND LABS針對2016年全球行動勒索病毒偵測統計圖[14]

常濫用的應用程式介面(API)受到更好的保護。當需要清除惡意程式時，現在也可以啟用裝置的root使用者和Android Debug Bridge(ADB)除錯橋接介面，或者開機進入安全模式，就可以清除惡意程式。使用者可採用一套多層式的行動安全防護來保護行動裝置，趨勢科技現行開發企業版行動安全防護工具可提供裝置、法規遵循與應用程式的管理，以及資料防護和組態配置，並可防止裝置遭到漏洞攻擊，避免存取未經授權的應用程式，還有偵測並攔截惡意程式和詐騙網站，表四為行動勒索病毒歸納；圖六為2016年全球行動勒索病毒偵測統計，圖七為變臉詐騙攻擊Limitless側錄程式產生器示意圖[15-16]。

圖七、變臉詐騙攻擊Limitless側錄程式產生器示意圖[16]

肆、資訊安全風險管理理論技術探討

事實上，針對於資訊安全風險議題進行探討時，良好風險管理對於單位組織取得長期穩定的成功至關重要，尤其面對日新月異的惡意程式攻擊，以及駭客入侵、社交工程、網頁掛馬、電腦病毒、資料外洩等資安威脅與日劇增，風險管理可以協助企業、單位組織避免資源浪費與損失，進而可改進營運作業流程提高作業效能並達到績效衡量管理等效益。目前，中國駭客的前五大攻擊目標分別為：資訊科技之智慧財產、航太相關事業(包括國防與空防)、政府單位、電信與衛星以及科學研究等單位。資安問題大多來自於「人」的問題，特別是單位的內部威脅，與供應鏈及科技人員，或者外包人員之安全查核與內部風險等均屬必要，建立嚴謹的安全分級制度刻不容緩。可參考美國建立情報諮詢委員會，在人員安全分級制度下，邀請民間部門參與，透明化監督制度，並且針對網路國安問題，首要加強國家關鍵基礎設施及其供應鏈的風險評估與強化。國家為提升國際資訊產業競爭力，積極投入資訊科技的研發及建置，行政院國家資通安全會報在2016年提出國家資通訊安全發展方案(102-105年)，期盼透過「推展資安基礎環境安全設定」、「加強資安防護管理二線監控機制及情蒐」、「強化資安應變功能及復原能力」及「建構資安專案管理(SPMO)機制」等52個行動方案，達成「強化國家資安政策，建立安全資安環境」

、「完備資安防護管理，分享多元資安情報」、「奠基資安技術能量，整合科技實務應用」及「擴大資安人才培育，加強國際資安交流」四大策略目標。行政院為建立可信賴的資通安全環境，確保資料、設備及網路系統的安全，保障民眾權益，建置政府專屬G-ISMS(Government- Information Security Management System)體系，以提升政府機關資通安全管理作業，妥善保護各機關資訊之機密性、完整性與可用性並建立機關聯防機制，降低資安事故之風險至可接受之程度。在複雜的網際網路環境中，因為資通安全是全方位的工作，必須就適法性、外在競爭環境的變遷、資產風險評估原則、資產價值，以及相關資訊服務等因素擬訂資安策略，不斷精進國家資安政策，投入相當資源，強化自我資通安全防護能力，建構國家整體性的資通安全服務環境，才能有效杜絕資安危害，維護國家資通安全。包含政府、關鍵基礎建設與企業分別透過加強資安應變及處理復原能力、推動政府機關資安管理制度、提升資安防護技術與軟體安全管理、培訓資安專業人才及國際交流合作等措施，預期可達成強化政府整體應變及處理能力、提供安心可信賴的資安服務、提升資安產業競爭力等目標[17-18]。

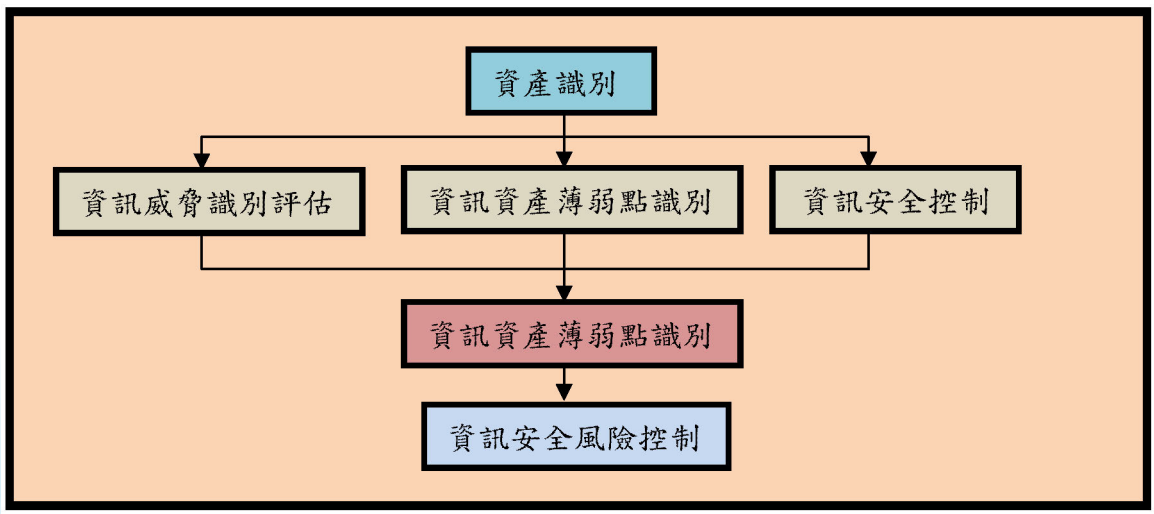
行政院國家資通安全會報技術服務中心報導分析，美國國家標準與技術研究院(National Institute of Standards and Technology，NIST)於2016年12月28日發布了「網路安全事件回復計畫」(Guide for Cybersecurity Event Recovery)，計畫編號NIST Special Publication 800-184，計畫重點在於五項重點(威脅識別、資訊安全防護、網路事件偵測、資安事件回應、落實完成回復作為)，目的訂定程序協助各個機構制定並實施網路安全事件回復作為，從而應對各類型可能的出現網路攻擊活動。此回復計畫強調，要成功應對網路安全事件，應建立資安事件處理三階段作業程序(事前安全防護、事中緊急應變及事後復原作業之具體機制)，尤其是包含關鍵資訊基礎設施(Critical Information Infrastructure，簡稱CII)，各組織機構需要提前制定自身的規劃與解決措施，確保團隊內部各成員了解籌備工作級別，瞭解相關具體角色與責任付予，並不斷重複演練。在訂定回復計畫時，完備文件需要包括有：相關設施單位組織同意書(同意包括備註外在回復支援團隊或相關協助需求)、單位主管授權(記錄至少兩員以上相關主管名字與聯繫方式)、組織回復團體成員(授權處理審核與演練相關計畫)、外部聯絡支援(以聯繫重要部門與資訊科技相關外部單位)、外部資料處理儲存中心(以方便儲存特定資料與媒體資料備援)、單位設施回復詳細內容(包括實地設施辦公室位置與資料中心相關回復資料記載)以及公共基礎架構(包括記錄基礎建設、軟體及硬體等身份管理系統登入，網路回復消息系統和臨時系統來驗證與確定從備份恢復數據的完整性)。網路安全事件回復

計畫的關鍵作用是有效預測可能發生影響的區域，定義影響等級與制定多功能計畫以減少損害。為實現以上功能，美國國家標準與技術研究院網路安全事件回復計畫(NIST Special Publication 800-184)需要下列組成要件，整理如下列表五[19-20]。

美國國家標準與技術研究院提出NIST Special Publication 800-184指引中還提供資料洩露網路安全事件範例，包括提供職能部門對應回復方案以及一套勒索軟體事件回復流程，並強調預測風險與完成詳細風險評估是網路安全事件回復計畫重要步驟。該指引期望透過正確制定並實施回復計畫、流程與程序，能夠幫助組織機構於遭遇網路攻擊後完全回復，並還原其安全性受打擊的系統以適合正式實施網路事件回復演練，並且詳細記錄結果以幫助通知組織網路安全活動，附錄A並備註回復作為網路事件回復計劃檢核表。值得注意的是，通過問題解決與相關演練，持續改進網路事件回復計劃，政策和程序在回復工作期間，並通過定期驗證回復功能。

表五、美國國家標準與技術研究院網路安全事件回復計畫組成要件說明

組成要件	網路安全事件回復計畫組成要件說明
權責區分完善計畫	強調須由組織的高階管理層主導訂相關事件回復計畫，以利計畫獲得所需動力，除此此外也需要清楚定義角色和責任管理程序
風險識別處理順序	預測風險是事件回復計畫成功關鍵，需要完成詳細風險評估，經由深入了解弱點，並確保其資訊安全風險正確識別以及處理順序
回復方法風險管控	針對資訊安全控管，特定的回復方法可以採取不同的形式，無論是硬體或軟體解決方案，資料庫備份，甚至通報管理機構均可，落實風險管理，對於每個潛在的事件都需要採取適當的後續處理
文件記錄詳實完備	詳細描述回復的操作步驟是回復計畫中核心，各部門詳細列出負責協助日常維運工作人員、流程及技術資產，加強資訊安全落實



圖八、資訊安全風險評估示意圖(自行整理)

這些活動並且包括具有具體作用和責任的現實目標行使和測試恢復能力，以驗證是否具備充分管理能力降低網路安全風險，並確保組織分析能源並將吸取經驗教訓納入相關計劃和過程。為了降低或消除資訊安全管理體系範圍所涉及到的被評估的風險，組織應識別和選擇適宜且合理的安全控制，透過實施安全控制使風險降低到組織可接受的程度，圖八為資訊安全風險評估示意圖[21-23]。

伍、結語與因應作為

依據趨勢科技全球技術支援與研發中心報導，在2016年企業資安高峰論壇中，美國聯邦調查局(FBI)督導特別探員(SSA)Timothy Wallach指出全球網路犯罪情勢及跨國駭客造成資安問題，由於網路犯罪來自世界任何地區，因此國際合作集體對抗犯罪將格外重要。除了與國際上的盟友分享資訊並協同調查，並且世界各地的探員也與駐在國合作，分析各項網路安全趨勢並掌握關鍵人員，落實資安管控，對敏感資料自動進行阻斷、隔離或加密，並監控可能洩漏重要資訊的資料型態。我們國家現行資安政策是透過資安人才培育、成立資安組織和制訂資安法規，讓資安因應與防護可以更臻完善，政府透過國家資安政策規畫，由國安會扮演政府國家層級高度的資安政策規定，委由行政院及跨部會落實並執行相關資安政策。2016年8月由國家安全會議和行政院召開的「資安即國安」策略會議中除了提醒資訊安全並非僅有技術層面的議題，並且強調透過整合資安人力、資安產業和科研資源，以提升資安基礎整備、產業能量和數位防衛能力，規劃目標達成包括：打造國家級的資安機制、建立國家級資安團隊確保數位國土安全、以及推動國防資安自主研發強化產業發展三大目標。面對資訊安全威脅，為能落實有效資安管控，單位組織資訊安全防護建議作為：定期備份重要資料，安全分級制應有明確的法律授權程序、範圍與監督機制，落實內部監督查核，並應嚴格執行各單位內部稽核制度，杜絕任何資安事件發生。建立早期預警系統、監控可疑連線及電腦、佈建多層次的資安防禦機制以達到縱深防禦效果、對內部敏感資料建立監控與存取政策及定期執行社交工程攻擊演練以強化資安危機意識[24-25]。

總而言之，政府機關加強防範措施強調：全面檢討網路及系統安全性、針對漏洞追蹤改善、成立網路安全小組訂定主機安全等級、加強資訊安全稽核、資訊單位定期進行弱點掃瞄、加強宣導人員對資訊安全的認知、提升系統管理人員資訊安全管理能力、加強網路安全管理、落實系統取存控制、存放機密與敏感性資料電腦主機不可連接到網際網路、資訊系統安全等級分類、加強資通安全軟硬體環境建置、並將重要資訊系統或資料從網際網路隔離出來，遠離惡意程式威脅以真正落實資安

管理與風險管控作為。面對勒索病毒與惡意程式攻擊資安威脅防禦分析，完善的備份措施是防範勒索病毒的首要步驟，其次是即時修補系統漏洞開啟自動更新，並且為能有效對抗勒索病毒與其他類型的攻擊，應該安裝病毒等惡意程式防護軟體完備資安防護作為，包括：運用入侵防護系統抵擋攻擊、安裝惡意程式防護軟體來防止系統遭到感染以及利用對外連線過濾來防止惡意程式連回伺服器。受到勒索病毒緊急措施切記：不要付錢，先立即切斷網路，避免將網路磁碟機或共享目錄上檔案加密。接著立即關閉電腦電源不讓勒索病毒繼續加密電腦中的檔案，關機時間愈快被加密的檔案愈少，建議強制關閉電腦電源，保留電腦並通報專業資安人員處理。針對資訊人員採取緊急處理措施步驟：暫時停用帳號，暫時停止該帳號的網路存取權限；檢查該帳號權限可寫入的共享資料夾是否遭受感染；取出硬碟，並透過另一台電腦備份尚未加密檔案。針對社交工程攻擊，電腦安全作為應注意上網習慣及防範透過電腦、手機洩露個人隱私資料，日常生活中需要培養資訊安全防範意識。對可疑電子郵件之自我保護措施：關閉預覽窗格、非必要閱讀之郵件逕行刪除、設定為純文字讀取模式再開啟郵件閱讀、開啟郵件內含超連結時確認連線網址網域名稱、若為數字IP之網址勿輕易開啟、不隨意輸入資料送出、傳送私密資料時確認是否有啟動加密機制。使用者在收取電子郵件時應注意檢查寄件者真偽、確認信件內容真實度、不輕易開啟郵件中超連結及附件及開啟超連結或檔案前確認軟體保持在最新修補狀態，強化資訊安全防範與健全網路危機管理觀念[26-27]。

陸、參考文獻

[1]趨勢科技全球技術支援與研發中心，2016年十大重大網路資安事件，趨勢科技資訊網，2017年2月20日。

[2]ITHome，Windows裝置小心!Mirai木馬程式來了，HiNet新聞網，2017年2月9日。

[3]趨勢科技全球技術支援與研發中心，從RAR到JavaScript：勒索病毒所使用郵件附件檔的變化，趨勢科技資訊網，2016年10月13日。

[4]TREND LABS趨勢科技全球技術支援與研發中心，五個網路NG行為，最容易幫詐騙集團爭取年終獎金，趨勢科技資訊網，2016年11月21日。

[5]TREND LABS趨勢科技全球技術支援與研發中心，平均每起變臉詐騙，企業損失逾430萬台幣一四個刷新紀錄的企業威脅，趨勢科技資訊網，2017年3月8日。

[6]TREND LABS趨勢科技全球技術支援與研發中心，Mirai殭屍網路成為鎂光燈焦點後，IOT物聯網威脅將成為主流，趨勢科技資訊網，2017年3月7日。

[7]趨勢科技全球技術支援與研發中心，何謂魚叉式網路釣魚(Spear Phishing)，趨勢科技資訊網，存取時間2017年3月8日。

[8]趨勢科技全球技術支援與研發中心，資安攻防新層次-趨勢科技2017年資安預測，趨勢科技資訊網，存取時間2017年3月8日。

[9]林妍溱，維基解密爆料：CIA以各種工具駭入手機、電腦及電視進行監控，電週文化，IThome資訊網，2017年3月8日。

[10]TREND LABS趨勢科技全球技術支援與研發中心，專挑MacOS的勒索病毒,Patcher假修補真加密,付贖金也無法挽回檔案，趨勢科技資訊網，2017年3月7日。

[11]Federico Maggi，《行動裝置勒索病毒》躲進口袋的壞東西:Android勒索病毒，一年增加了140%，Mobile Ransomware: Pocket-Sized Badness，趨勢科技資訊網，2016年12月30日。
[12]TREND LABS趨勢科技全球技術支援與研發中心，五大行動裝置勒索病毒家族成長率屢創新高，趨勢科技資訊網，2017年2月17日。
[13]Trend Micro Senior Threat Researchers，Not so Limitless after all: Trend Micro FTR Assists in the Arrest of Limitless Author，趨勢科技資訊網，2017年1月19日。
[14]Unwire Pro，現今網路勒索軟體威脅，CryptoWall、Locky與Cerber名列前3名，科技新報TechNews，2016年6月11日。
[15]Lord Alfred Remorin，認識變臉詐騙/BEC-(Business Email Compromise)商務電子郵件詐騙與防禦之道，Change of Supplier Fraud: How Cybercriminals Earned Millions Using a $35 Malware，TREND LABS趨勢科技全球技術支援與研發中心，2016年2月2日。
[16]趨勢科技資訊網，BEC變臉詐騙男大生認罪,利用Limitless鍵盤側錄程式危駭數千企業!趨勢科技FTR團隊協助逮捕，趨勢科技資訊網，2017年2月9日。
[17]行政院國家資通安全會報，資通安全資訊網，國家資通訊安全發展方案(102-105年)，2016年2月2日。
[18]行政院研考會，資訊系統風險評鑑參考指引(修訂)v2.0，2017年03月05日存取。
[19]財團法人台灣智庫，國會政策研究中心，關鍵基礎設施安全條例(CIIP)—國家資通安全的第一哩路，2017年3月10日存取。
[20]財政部財政資訊中心，財政部暨所屬機關(構)資訊安全管理準則，2002年6月訂頒，http://www.fia.gov.tw/，2017年03月05日存取。
[21]行政院國家資通安全會報技術服務中心，美國NIST發布網路安全事件回復指引，國家資通安全會報資通安全資訊網，2017年1月13日存取。完整網路安全事件回復指引內容請參閱：http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf
[22]Trend Labs趨勢科技全球技術支援與研發中心，勒索病毒把網友當搖錢樹?三步驟保護自己，2017年02月10日。
[23]行政院國家資通安全會報，2016年全球勒索軟體攻擊次數激增，國家資通安全會報資通安全資訊網，2017年3月5日存取。
[24]黃彥棻，【資安周報第63期】尋找臺灣資安新動能系列報導(四)：國家安全會議諮詢委員李德財要從國安高度推資安3箭，保護臺灣數位國土，電週文化，IThome資訊網，2017年3月7日。
[25]行政院國家資通安全會報技術服務中心，請注意！工業與環境控制設備無身份驗證機制或使用預設密碼，並曝露於網際網路上，恐有資訊外洩與遭受入侵之疑慮，資通安全資訊網，2017年02月17日。
[26]行政院國家資通安全會報技術服務中心，資通安全資訊網，資通安全辦公室，國家資通安全通報應變作業綱要(修正版)，2017年03月05日存取。行政院國家資通安全會報國家資通安全通報應變作業綱要-內容請參閱：www.nicst.ey.gov.tw/Upload/UserFiles/國家資通安全通報應變作業綱要.pdf
[27]洪羿漣，勒索詐騙攻擊防不勝防，用機器學習增益端點安全，新技術結合長期累積情資-終端資安防護強調跨世代，電城邦文化事業，Net Admin網管人資訊網，2017年3月20日。

作者簡介

空軍備役上校　吳嘉龍

學歷：中正理工學院48期電機系電子組、美國空軍理工學院電腦工程研究所、國防大學理工學院國防科學研究所電子工程組。經歷：電子官、區隊長，教官、講師、助理教授、科主任、校教評秘書、副教授、教授、系主任、圖書館館長、資圖中心主任。現職:航空技術學院一般學科部航空通訊電子系兼任教授。專長領域：資訊戰、通資安全、無線通訊、網路通訊協定、危機管理。