上網行為安全
-網路駭客遠離我

資安顧問　　郭洛坤

講師簡介

- 郭洛坤 Damon Kuo
- Experience
  - 漢昕科技 資安顧問
  - 樹德科技大學 兼任講師
  - 國家高速網路與計算中心 助理研究員
- Certified :
  - BS 10012:2009 LAC (PIMS)
  - CEH (Certified Ethical Hacker)
  - ECSA(EC-Council Certified Security Analyst)
  - CHFI(Computer Hacking Forensic Investigator)
  - ISO 27001:2005 LA (ISMS)
  - ISO 9001:2008 LA (QMS)
  - ISO 20000:2011 LA (ITSMS)
- Contact: damon@bccs.com.tw

- 授課/演講單位(時數500+) :
  - 經濟部加工出口區管理處
  - 國立海洋生物博物館
  - 台灣自來水公司
  - 高雄市政府
  - 高雄市警察局
  - 高雄市政府地方稅務局
  - 高雄縣政府地方稅務局
  - GETRIGHT SOLUTIONS COMPANY(MALAYSIA)
  - 聚和國際股份有限公司
  - 高雄應用科技大學
  - 高雄第一科技大學
  - 中華醫事科技大學
  - 樹德科技大學
  - 國立中山大學附屬國光高級中學

大綱

- 社交工程攻擊
- 最新資安情勢
- 勒索軟體威脅

社交工程攻擊

何謂社交工程

- 社交工程(Social Engineering)使用的方法不是依靠資訊技術，而是一種利用人性弱點的詐騙技術，可以藉由與他人之間的互動，或利用某些組織內部的人員去違反組織的政策，最後的目的就是獲得有價值的敏感資訊。

郵件社交工程

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法
- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊
- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

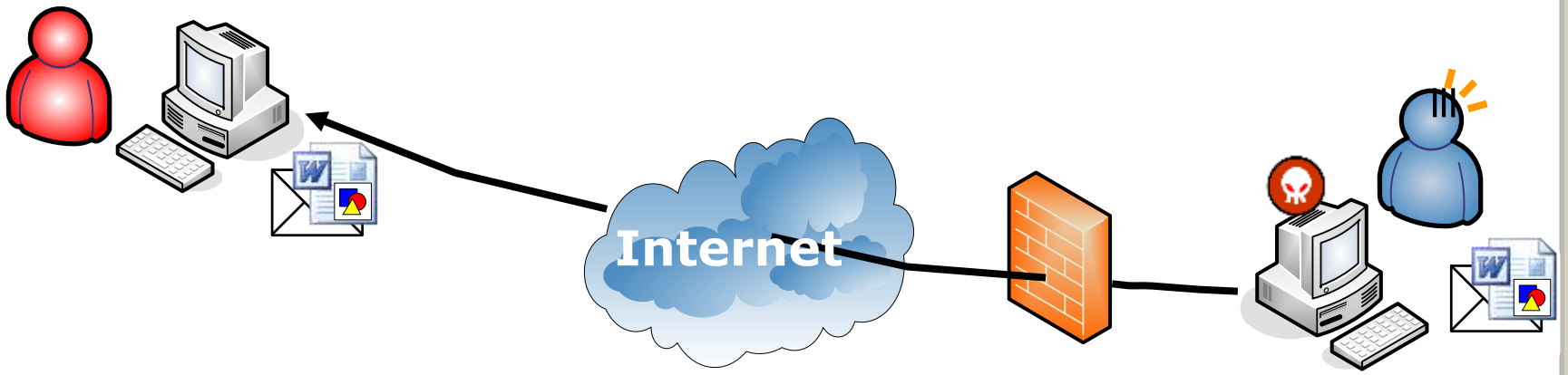
網路駭客手法

- 一、註冊相似度極高之網域名稱：
  - 駭客利用網路申請註冊網域名稱之便利性，利用極為相似之字母或數字，如英文字母小寫l與數字1，n與h等極為相似之符號以假亂真，使國外客戶難以辨別使用者(user)名稱之後真偽。
  - 或維持使用者(user)名稱，直接以相似度極高之網域名稱代替。例如：駭客將lisalin@yahoo.com網域名稱變更，改成lisalin@ymail.com。
- 二、植入木馬程式：
  - 駭客利用暗藏的惡意或木馬程式，包括遠端遙控功能及鍵盤側錄程式，側錄民眾上網時所輸入之帳號密碼，並搜尋電腦所有磁碟是否存有憑證檔案，再將憑證及鍵盤操作紀錄之帳號密碼遠端傳送回駭客的主控台，因而得以輕易破解電腦保護措施，取得民眾電子信箱之帳號密碼，入侵電子郵件後竄改郵件內容。
- 三、進行客製化犯罪行動：
  - 犯罪集團入侵電子郵件信箱後，會針對公司做極為詳盡的資料蒐集，包括監控臺商與客戶間之對話，包括客戶之姓名、公司電話、電子郵件帳號及銀行帳號等，再利用非法取得之資料，運用社交攻擊手法，更進一步取得各種如網路銀行、行動電話等客服及語音電話服務所需之個人身分驗證資料，以「假冒客戶」通過客服人員所提問之身分驗證資訊，籍此「套出」更多個人隱私資料，進行各種假冒身分之犯罪詐騙行為。

民眾防制作為

- 一、注意密碼設定：
  - 密碼設定至少要有英文、數字與特殊符號等，且經常更換密碼，以免帳號密碼遭盜用。
- 二、檢查郵件寄件者：
  - 將滑鼠游標移到寄件者名稱上，看看顯示名稱與寄件者名稱是否相符，尤其須特別留意電子郵件使用者名稱(user name)及網域名稱(domain)是否有異。
- 三、加強客戶端之安全檢核機制：
  - 請國內企業多加注意，如能多幾個方式和客戶端再次確認匯款銀行及帳戶之正確性，將能多一份保障，以避免造成重大財損。
- 四、使用正版軟體與使用防毒軟體：
  - 企業電腦安裝正版軟體，隨時或定期上網修補系統程式漏洞，確保企業電腦安全，並確認企業電腦安裝正版防毒阮體，以提供一定程度的安全防護。

郵件社交工程攻擊模式



1. 駭客設計攻擊陷阱程式(如特殊 *Word* 檔案或外部惡意連結)
2. 將攻擊程式置入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，將被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

偽造攻撃

偽造攻擊

- SMTP 通信規範, *沒有辦法限制驗證寄件人的身份*. 雖然可以用身份驗證機制確保信是由特定人員寄出(例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...

- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的

- 整封信件，都是假的!!!!!!!!

退信攻擊

退信攻擊

- ***收件人不存在導致無法送達郵件***，就會自動將該***退信訊息寄回給原寄件者***
- 利用這項功能，使用*字典攻擊所蒐集到的Email*
- 將***欲攻擊的對象設定為寄件者***
- ***收件者使用其他單位不存在的帳號***
- 然後你就會收到一封***不是自己寄出去的退信***了

跳板攻擊

跳板攻擊

- 當您的*電腦主機本身有啟用SMTP Service* (外寄伺服器服務)，而且*沒有加以防護*時，被有心人士發現，進而不當使用您的網路頻寬及寄信功能，濫寄廣告信件，這就是您的電腦主機被當成廣告信跳板了!!
- 通常受害者不知道自己的電腦安裝了相關服務
- 常見微軟的作業系統，當有*安裝了IIS功能*，*就會一同安裝SMTP(外寄伺服器服務)*，此時若您的網路系統並未安裝防火牆，將 SMTP PORT 25 設為對外阻隔的話 ，基本*上任何人都可以藉由您的 SMTP Service 寄發信件*!! 您的電腦主機，就有可能被有心人士當成廣告信跳板，濫寄廣告信件!!

Case Study

HBGary Company Inc.

郵件社交工程
防護停看聽

收信軟體安全性設定

- 以微軟的outlook express收信軟體為例，建議進行以下安全性的設定：
  1. 取消「郵件預覽」
  2. 取消「在預覽窗格檢視郵件時自動下載郵件」
  3. 勾選「以純文字閱讀所有郵件」
  4. 設定安全性區域為「受限制的網站區域」
  5. 勾選「在其他應用程式試圖以我的名義傳送電子郵件時警告我」
  6. 勾選「在附件有可能有病毒時不允許儲存或開啟」
  7. 勾選「阻擋HTML電子郵件中的圖片和其他外部內容」

防騙停看聽

停	安裝防毒軟體，確實更新病毒碼 關閉信件自動下載圖片及其他內容 以純文字模式開啟信件 取消信件預覽功能 設定過濾垃圾郵件機制
看	信件是否來自政府單位(gov.tw)或教育單位(edu.tw) 標題或內容是否與本身業務相關 其餘信件應視為垃圾郵件
聽	透過電話向對方確認信件真偽 透過電子郵件再次確認

最新資安情勢

郵件門

郵件門

Investigations

How Clinton's email scandal took root

By Robert O'Harrow Jr. March 27

This article reflects a revised number for the FBI personnel working on the Cli
email case. Correction at conclusion of story.

Hillary Clinton, who at the time was selected to be secretary of state, checks her BlackB
on an elevator at the U.S. Capitol in the District in January 2009. (Chip Somodevilla/Get
Images)

Hillary Clinton's email problems began in her first days as secretary of state.
insisted on using her personal BlackBerry for all her email communications, l
she wasn't allowed to take the device into her seventh-floor suite of offices, a se
space known as Mahogany Row.

BBC 登錄 選項（英文）

中文网

主頁 | 國際 | 兩岸 | 英國 | 評論 | 科技 | 財經 | 圖輯 | 音頻材料 | 視頻材料 | BBC英倫網

美國大選：郵件門調查重啟 希拉里要求解釋

2016年 10月 29日 分享

希拉里的支持率仍然高於特朗普

為什麼會有郵件外流

- 希拉蕊有兩個習慣
  - 習慣看紙本信
  - 習慣用有鍵盤的手機(黑莓)
- 可是呢
  - 她有一個得力助手胡瑪·阿貝丁（Huma Abedin)，負責幫她把信弄成紙本。
  - 任國務卿時，國務院因為”資安規定”，列印紙本是非常麻煩的事。
  - 透過基金會名義申請了幾個域名(clintonemail.com、wjcoffice.com、presidentclinton.com等,申請人為Eric Hoteham,希拉蕊前助手)

為什麼會有郵件外流

- 可是呢(cont.)
  - 阿貝丁在柯林頓家地下室弄了兩台MAC Server(Outlook exchange)，當作郵件伺服器，並且將信件列印成紙本供希拉蕊閱讀。
  - 而後這些伺服器被轉到一家叫Platte River的資訊公司。
- 另一方面
  - 因為班加西事件(13Hour)後，多方勢力想要拿到希拉蕊下指示的信件。

郵件外流的關鍵點

- 班加西事件在201510接受國會的聽證會調查後希拉蕊獲得不起訴的處份。
- 引來維基解密-朱利安.阿桑奇的不滿，釋出相關文件約20000筆信件。來源為民主黨公關主任等七位重要官員。
- FBI調查結果發現無實質證據，但說明有33000封被刪除的信件無法取得。
- 201607民主黨資料總監在自家門口被槍殺。

郵件外流的關鍵點

- 希拉蕊的競選經理John Podesta，點到了一封釣魚郵件，大量信件外流。黑客把信件內容交給維基解密。
- 201610阿貝丁的前夫，安東尼.韋納(Anthony Weiner, 紐約州前民主黨議員)，因為曾對15歲女孩發過色情短信，引來監控兒童色情犯罪的FBI調查。
- 韋納的電腦裡發現662781封信件，其中有11112封是阿貝丁的，其中有一部分是希拉蕊的，而且是先前被刪掉33000封中的一部分。

郵件外流的關鍵點

- 20161028，mega老闆Kim Dotcom說他知道那33000封信在猶他州NSA內部的spy cloud上。

- 20161029，FBI局長科米宣布重啟郵件門調查。

這個案例我們學到什麼？

- 希拉蕊犯了什麼錯？
- 嚴重嗎？
- 怎麼做才避免？

宣導一下

- 行政院及所屬各機關資訊安全管理要點第 27 條：「各機關應訂定電子郵件使用規定，機密性資料及文件，不得以電子郵件或其他電子方式傳送。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關應視需要以適當之加密或電子簽章等安全技術處理。機關業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。」

DDoS勒索

DDoS手法

- 網路層
  - 目標：癱瘓頻寬
  - UDP / ICMP Flood、Reflection & Amplification
- 系統層
  - 目標：癱瘓基礎建設或系統層
  - SYN / ACK Flood、Fragment Packet Flood、Connection Flood...etc
- 應用層
  - 目標：癱瘓應用服務
  - SSL Flood、HTTP Flood、DNS Flood、Exploit、Slow Attack...etc

DDoS實例

- 某國19家證券商聯合被DDoS勒索比特幣案例(2017/02)
  - 第一波800Mbps攻擊流量，某券商就倒了(頻寬不足)。
  - 第二波平均2Gbps攻擊流量，每秒約700k封包，時間2x分鐘，最長有1小時。
  - 手法為NTP放大與反射攻擊、UDP Flood、ICMP Flood洪水攻擊。
  - 來源95%境外，50%為美國海纜介面來源。

DDoS防禦現況

- ~~防火牆~~

- 外部
  - 頻寬 / 多線路 / 多資料中心 / CDN
  - 流量清洗服務

- 本地
  - 防護設備(IPS...etc)
  - 系統調校人員
  - 錄封包分析

本地DDoS防禦現況

- 網路層
  - 辨識特徵+過濾(IP/PORT/ID/TTL/SEQ/ACK…etc)
- 系統層
  - 辨識特徵+過濾(SSL/URL/Parameter/User-Agent/Referrer/Cookie…etc)
  - 設備調校(加(換)設備、關掉負載高的功能或模組、調參數降低攻擊影響)
- 應用層
  - 增加服務能量、減少異常存取
  - Redirection / Challenge / Authentication

IOT安全

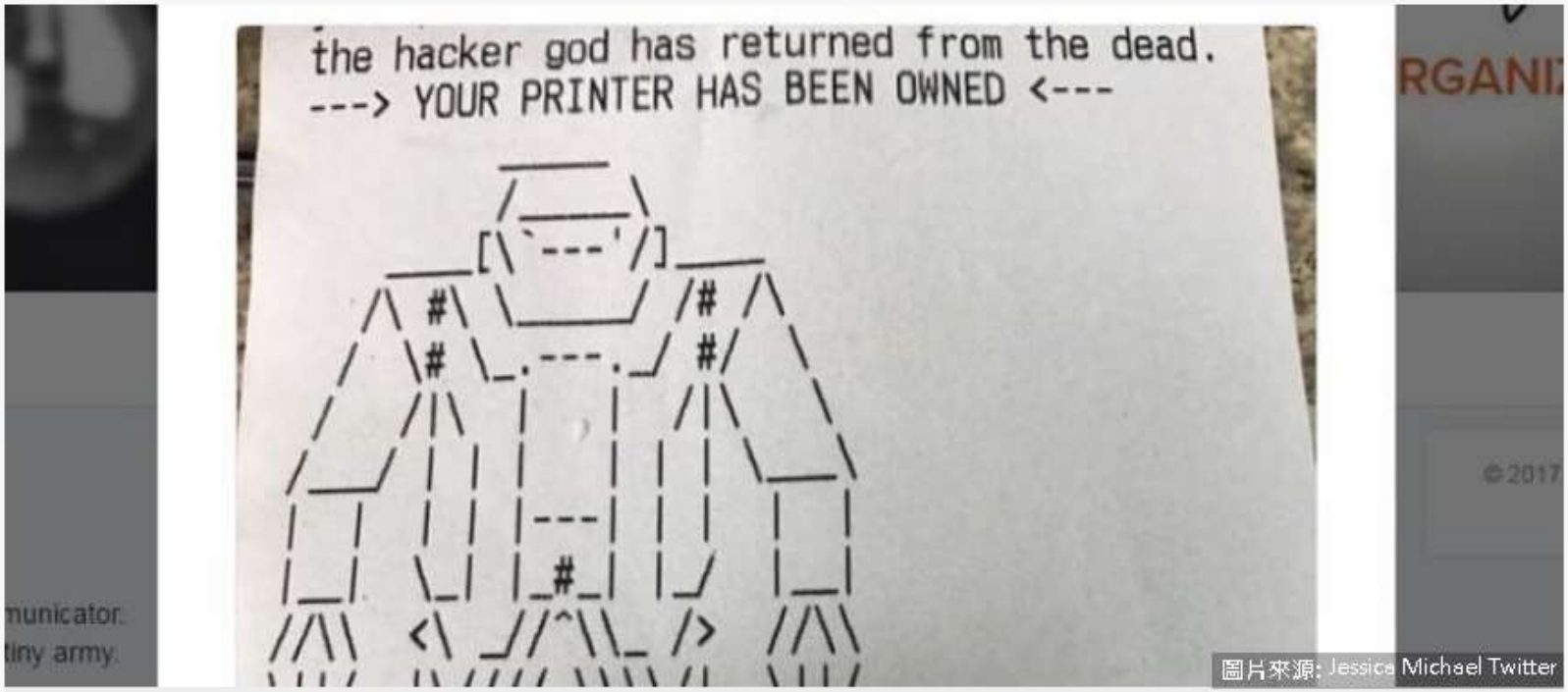
Printer

別輕忽印表機安全，白帽駭客入侵15萬台網路印表機示警

為喚起外界重視印表機安全，署名為Stackoverflowin的白帽駭客上周入侵15萬台網路印表機，遙控這些印表機列印出文字及圖案訊息，包括Canon、Epson、HP、Lexmark到Brother等主要品牌均受影響。

文/ 陳曉莉 | 2017-02-06 發表

按讚加入iThome粉絲團



圖片來源: Jessica Michael Twitter

用戶在推特上反映印表機遭遙控印出文字與ASCII圖案。

你以為印表機很安全嗎? 全臺46所學校印表機遭駭客入侵！

POSTED ON 2017 年 03 月 10 日 BY 165反詐騙

Share

2017年資安風暴一波未平一波又起，上個月二月初臺灣證券市場才遭逢第一件大型駭客攻擊，二月底多所學校的網路印表機均收到自動列印署名為Emerson Rodrigues之恐嚇信件，要求校方指定時間前支付3個比特幣（約新臺幣10萬元），若未準時付款就會於3月1日發動網路攻擊以癱瘓學校網路。

延伸閱讀>>臺灣證券市場遭逢第一件大型駭客攻擊！刑事局已介入偵辦

經過教育部調查後，上週五至本周一為止，全臺已有多達46所學校收到駭客威脅信，目前以大專院校為大宗。仍有部分縣市尚未回報，估計受駭客入侵學校數量恐怕不只如此。根據行政院國家資通安全會報公告，該類印表機因曝露於網際網路且未設置相關登入帳號密碼或使用預設密碼，導致有心人士可於外部直接存取網路印表機。

IP CAM

- http://www.insecam.org/

http://www8.hp.com/tw/zh/solutions/security/thewolf.html
https://www.youtube.com/watch?v=FqibWHfn_Yc

勒索軟體

什麼是勒索軟體?

01
- 視為病毒或惡意程式
- 透過各種感染途徑，讓電腦有惡意程式執行...

02
- 對檔案進行不可預期行為
- 對使用者常用的格式，進行加密動作...

03
- 要求受害者付出贖金
- 錢能夠解決的都是小事...

04
- 期待又怕受傷害
- 好一點的勒索病毒還有保證期間，免費優待解鎖...

- 其他惡意程式
  - 來自隨身碟
  - 弱點攻擊
- 電子郵件
  - 夾帶惡意程式的文件檔
  - 腳本程式
  - 釣魚連結
  - 廣告郵件
- 網際網路
  - 遭到入侵的網站
  - 釣魚網站
  - 惡意廣告

勒索軟體運作

- **第六階段**

交易完成，駭客會將解密方式給予受害者

- **第四階段**

顯示勒索訊息給受害者

- **第二階段**

勒索軟體執行運作

- **第五階段**

受害者**支付贖金**並附上交易序號給駭客

- **第三階段**

搜尋特定檔案將其**加密**或其他動作

- **第一階段**

透過各種階段進入受害者電腦

加密運作進行方式

01	02	03	04
■ 進入電腦開始運作 ■ 至網路下載加密金鑰	■ 搜尋常用文件檔案 ■ 例如JPG、DOC等常見類型	■ 針對檔案進行加密動作	■ 檔案開頭有加密金鑰 ■ 留下聯絡資訊

贖金付款方式

01	02	03	04
■ 受害者電腦顯示訊息 ■ 指示付款方式與款項	■ 購買指定的錢幣，如比特幣、乙太幣等 ■ 匯款至指定戶頭 ■ 約3~500美元或以上	■ 依照指示給予交易序號 ■ 證明付款無誤	■ 收取解密金鑰與步驟 ■ 通常為兩支程式，A程式解開本機某個金鑰檔(key值)。 ■ B程式套用Key值至被加密的檔案(還原出原檔)。

加密方式解析

對稱加密

對稱解密

- RSA 2048 加密演算法
- 一經加密無法破解
- 除非有對應解密金鑰

非對稱加密

加密金鑰

非對稱解密

解密金鑰

勒索軟體處置

- 緊急處置(發現勒索軟體正在加密)
  - 中斷網路
  - 立馬關機
  - 不要點選已加密的檔案
  - 保持現場，請求支援(鑑識/重置)

- 平時處置
  - 重要檔案定期備份(一份備不夠，你有沒有備兩份？)
  - 備份檔案不要以磁區型式連線(隨身碟/網路磁碟機)
  - 防毒軟體定期更新。
    - Bitdefender Anti-CryptoWall (僅針對Cryptowall)

勒索軟體處置

- Kaspersky
  - https://noransom.kaspersky.com/
  - 針對CoinVault、Bitcryptor兩款進行私鑰解密運算。
- FireEye/FoxIT
  - http://www.decryptcryptolocker.com/
  - 透過逆向工程取得金鑰，僅針對CryptoLocker(不含其變種)。

勒索軟體處置

- Bitdefender
  - http://labs.bitdefender.com/wp-content/plugins/download-monitor/download.php?id=Decrypter_0-1.3.zip
  - 針對Linux平台的Linux.Encoder.1進行破解。
- 你中的勒索軟體版本不在上列？
  - 付錢是一條路。
  - 但付錢也不保證能拿得到金鑰。

防護方式

- 修補弱點

- FLASH更新
- IE更新或改用chrome、firefox

- 防毒防火牆

- 安裝防毒軟體或防火牆監控
- 安裝廣告軟體阻擋程式

- 提高警覺性

- 不明程式、郵件或不熟悉網站不要點/執行
- 再次確認避免中招

- 備份

- 平時勤備份
- 雲端硬碟(如google drive)是好幫手

可疑檔案上傳分析：

- 利用各家防毒軟毒軟體的掃描引擎，同時對單一一個檔案，作是否為病毒、木馬檔案的分析可協助檢測確認檔案本身是否異常。
- Virus Total
  - 整合型線上惡意程式掃描
  - 網址:https://www.virustotal.com/
- VxStreamSandbox
  - 惡意程式分析網站
  - 網址:https://www.hybrid-analysis.com
- Malrw
  - 惡意程式分析網站
  - 網址:http://malwr.com

案例3 Wannacry

THE Sun | OTBALL | SPORT | TV & SHOWBIZ | NEWS | LIVING | MONEY | MOTORS

PATCHING THINGS UP **What is Microsoft's MS17-010 Windows patch and how can you protect your PC from Wannacry ransomware?**

The technology company has released a critical security update for users operating an old Windows system

By Gemma Mullin

15th May 2017, 10:18 am | Updated: 15th May 2017, 5:43 pm

1 COMMENTS

MICROSOFT was forced to act quickly after more than 200,000 computers around the world were subject to a massive cyber attack.

It came amid concerns networks were left vulnerable because they were still using outdated Windows XP software.

Wannacry

- 基於永恆之藍(EternalBlue)漏洞利用程式擴散的加密型勒索軟體兼蠕蟲病毒(Encrypting Ransomware Worm)。
- 2017/4/14，該(批)漏洞由Equation Group泄露，並由Shadow Brokers披露，據信Equation Group為NSA組織。
- 2017/5/12開始攻擊，第一波攻擊超過99國，最終超過150國受害。主要利用SMB協定進行擴散。
- 此一漏洞早先於2017/03/14已發佈更新(MS17-010)。

Wannacry 花絮

- 因為會檢測是否為沙箱OS，所以會呼叫www.Iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com網域，若有回應則不觸發(kill switch)；後英國工程師註冊該網域後第一波攻擊減緩。
- 中國地區因金盾擋掉該網域，故成為第一型病毒肆虐最久的國家。

有解否

- 由於正確的使用了Windows Crypto API，所以解密需要兩個條件
  - 受害電腦未重置(重開機)
  - 特定記憶體位置未被其他程序覆寫
- 解藥 WanaKiwi
  - 加密需要私鑰/公鑰，wannacry加密後會刪除密鑰。
  - 但未釋放記憶體前不會刪除記憶體中的prime number
  - WanaKiwi透過搜尋記憶體中的prime number重建密鑰。

你該如何自保？

- 使用者
  - 確保所有的軟體處於最新版本
  - 提高信箱密碼複雜度並定期更改
    - 11碼混合英數字大小寫
    - 8碼混合英數字大小寫及符號
    - GCB建議:60天更換，12碼英數字大小寫及符號
  - 減少提供過度的資訊給網路服務
  - 避免在多個網路服務中共用密碼
  - 定期備份，並保持至少一份檔案為離線備份
  - 留意你的網路使用行為
    - 任意平台的附件與連結

Summary

- 社交工程攻擊
- 最新資安情勢
- 勒索軟體威脅

問題 與 討論