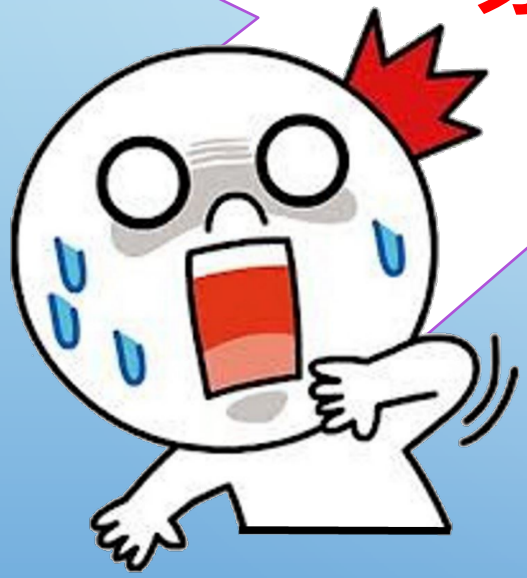
WANACRY PT0R 2.0勒索病毒

WANACRYPT0R 2.0 攻擊系統漏洞

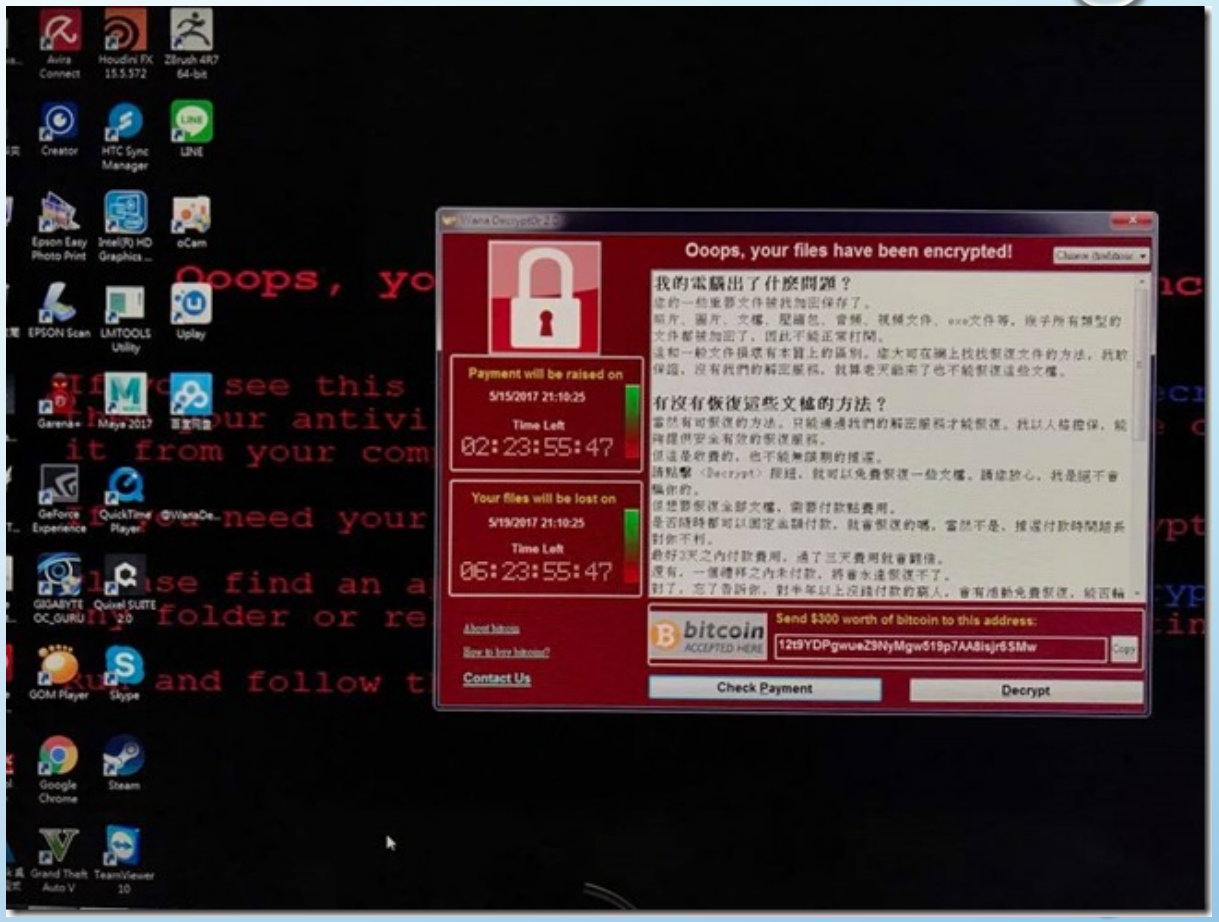
台灣成全球第二大勒索病毒受災國家



WANACRYPT0R 2.0 透過系統漏洞攻擊

特色是：

1. 不知道為何中毒，沒有去奇怪的網站。
2. 檔案的副檔名被更改為 .WNCRY。
3. 受災戶大多坐落在 WIN 7 的使用者。
4. 中毒提示視窗為紅色邊框，有多國語言版本可以選擇。



病毒名為「WanaCrypt0r 2.0」，其索取金額高達 300 美金，透過內容訊息可以得知，勒索病毒作者要求在三天內付款，三天一到就是翻倍贖金，而如果一到七天，檔案就會永久無法刪除。

使用攻擊漏洞的方式來進行病毒的散播

- 漏洞編號為 MS17-010(CVE-2017-0143~CVE-2017-0148)，駭客可以透過這個漏洞遠端在你的電腦上執行程式碼
- 會被此漏洞影響到的作業系統有
  - WINDOWS VISTA、7、8、8.1、10(1507,1511,1607)
  - SERVER 2008、2008 R2、2012、2012 R2、RT。
- 不過此漏洞已經在 3月安全性更新（2017 年 03 月 14 日發布）中有做修補了。

Microsoft 資訊安全公告 MS17-010 - 重大

Microsoft Windows SMB 伺服器的安全性更新 (4013389)

發行日期：2017 年 3 月 14 日

版本：1.0

提要

本頁內容

受影響的軟體和弱點嚴重性等級

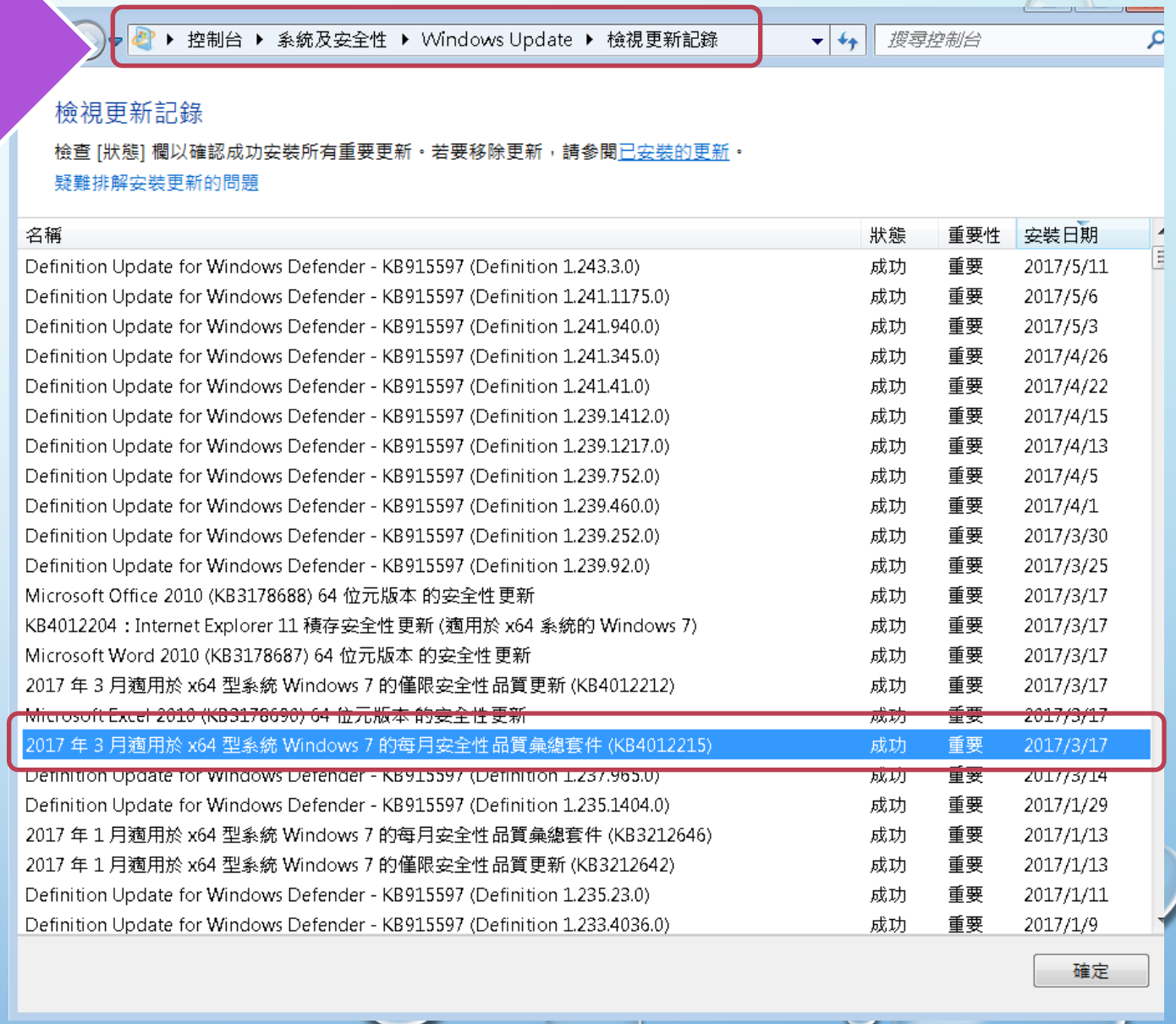
- 這一批勒索病毒是針對WINDWS 作業系統的SMB(445 PORT漏洞)來攻擊
- **W7(KB4012215)、W8.1(KB4012216)還沒中毒的用戶趕快去下載**
- ----------

1. 目前這已知最新版W10(1703版)沒有這個BUG，所以不會中該隻病毒
2. 下載安裝後如出現「此更新不適用於你的電腦」
   - 建議去「控制台\系統及安全性\WINDOWS UPDATE\檢視更新記錄」
   - **找有沒有 KB4012215 OR KB4012216，如果有就不用擔心了**
   - 如果沒有，那你可能是W7版本太舊，直接透過WINDOWS UPDATE更新
3. W10用戶如果還沒升級1703，直接更新就好..
4. XP應該也有這個BUG，但是目前沒看到MS有KB可以補。

- ----------

檢查到底有更新了嗎?

- 目前學校內的電腦除了去年更換的ASUS MD580為Windows 7-64位元
- 其他皆為Windows 7-32位元。
- **沒有怎麼辦？趕緊到Windows Update更新。**

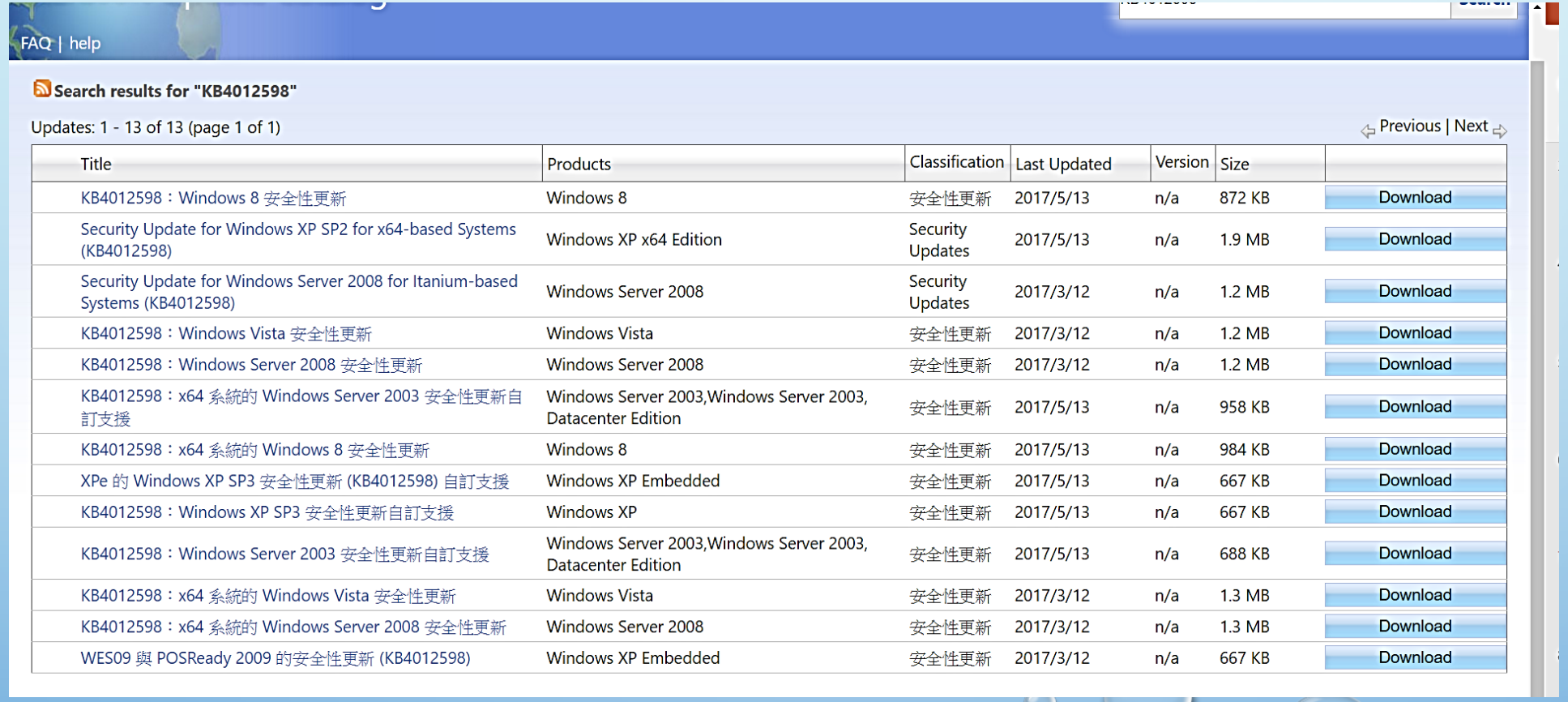


如何知道WINDOWS10的版本

- 點選[開始(WINDOWS視窗)
- 找到[設定]隨便選一個
- 找到[關於]
- 就可以知道你目前WINDOWS 10是哪個版本

WINDOWS 7以前版本更新檔下載位置

- http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598。



FAQ | help

Search results for "KB4012598"

Updates: 1 - 13 of 13 (page 1 of 1) Previous | Next

Title	Products	Classification	Last Updated	Version	Size	
KB4012598：Windows 8 安全性更新	Windows 8	安全性更新	2017/5/13	n/a	872 KB	Download
Security Update for Windows XP SP2 for x64-based Systems (KB4012598)	Windows XP x64 Edition	Security Updates	2017/5/13	n/a	1.9 MB	Download
Security Update for Windows Server 2008 for Itanium-based Systems (KB4012598)	Windows Server 2008	Security Updates	2017/3/12	n/a	1.2 MB	Download
KB4012598：Windows Vista 安全性更新	Windows Vista	安全性更新	2017/3/12	n/a	1.2 MB	Download
KB4012598：Windows Server 2008 安全性更新	Windows Server 2008	安全性更新	2017/3/12	n/a	1.2 MB	Download
KB4012598：x64 系統的 Windows Server 2003 安全性更新自訂支援	Windows Server 2003,Windows Server 2003, Datacenter Edition	安全性更新	2017/5/13	n/a	958 KB	Download
KB4012598：x64 系統的 Windows 8 安全性更新	Windows 8	安全性更新	2017/5/13	n/a	984 KB	Download
XPe 的 Windows XP SP3 安全性更新 (KB4012598) 自訂支援	Windows XP Embedded	安全性更新	2017/5/13	n/a	667 KB	Download
KB4012598：Windows XP SP3 安全性更新自訂支援	Windows XP	安全性更新	2017/5/13	n/a	667 KB	Download
KB4012598：Windows Server 2003 安全性更新自訂支援	Windows Server 2003,Windows Server 2003, Datacenter Edition	安全性更新	2017/5/13	n/a	688 KB	Download
KB4012598：x64 系統的 Windows Vista 安全性更新	Windows Vista	安全性更新	2017/3/12	n/a	1.3 MB	Download
KB4012598：x64 系統的 Windows Server 2008 安全性更新	Windows Server 2008	安全性更新	2017/3/12	n/a	1.3 MB	Download
WES09 與 POSReady 2009 的安全性更新 (KB4012598)	Windows XP Embedded	安全性更新	2017/3/12	n/a	667 KB	Download

美國《消費者報告》網站也提供5招降低中標的招式

1. **不要隨意點擊電子郵件中的連結**，而是在瀏覽器輸入網址。
   - 如果不知道官網網址，請用GOOGLE搜尋。
2. **不要打開附件**，除非你確認內容安全，也知道內容為何。
3. **不要訪問可疑的網站**，例如盜版下載網、色情網站，這些網站很容易受攻擊。
4. **不要隨意下載軟體**。
5. **要定期將重要的檔案和資料備份**，就算中標，損失也不至於太大。
6. **定期更新(作業系統、防毒軟體、相關軟體)**<---小弟加的

相關更新

- Windows更新：請不要關閉windows update，一般來說當有相關更新，在你按下左下角[視窗]選擇[關機]時會看到盾牌，或許會需要時間，但請耐心等候就是了。
- Chrome更新：按下右上角[…(直的)]選擇[說明][關於Google Chrome]就會檢查版本和更新，更新完重新啟動CHROME即可。
- Adobe Flash更新：如果擔心請連到官網[https://get.adobe.com/tw/flashplayer/]去下載更新。

- **不管是更新還是安裝軟體，如果軟體出現要安裝其他的軟體，建議都不要安裝。**

- 另一篇關於勒索病毒的報導

重大資安事件 > 勒索病毒 RANSOMWARE /勒索軟體(CERBER,CRYPTOLOCKER ...)

“ADOBE FLASH 版本太舊需要更新?” 按下後卻中了勒索病毒

- 遠離6 種更新通知陷阱

ADOBE FLASH 版本太舊需要更新.....

- 最近有網友反應 ,上網時忽然跳出通知說 ADOBE FLASH 版本太舊需要更新,不疑有它按下後就中了勒索病毒。本文要告訴你有哪些更新通知,其實暗藏陷阱,尤其是勒索病毒,畢竟電腦可以重灌,那些年的照片卻無法重拍.....
- 《延伸閱讀》收到 FACEBOOK訊息的 ADOBE FLASH更新影片,請當心是詐騙!!

LOCKY 勒索病毒利用 FLASH 和 WINDOWS 系統核心漏洞散播,

- 英國獨立報紙 THE INDEPENDENT 網站曾因遭到入侵，使得瀏覽其網站的使用者都被重導到專門感染 ANGLER 漏洞攻擊套件的網站。此時，使用者電腦上的 ADOBE FLASH PLAYER 若非最新版本，其電腦就會被植入 TESLACRYPT 勒索病毒。類似 LOCKY 勒索病毒利用 FLASH 和 WINDOWS 系統核心漏洞散播,類似這樣的事件時有所聞,保持作業系統、ADOBE FLASH、瀏覽器等重要軟體更新是防範漏洞攻擊、保障系統安全的方式之一,但趨勢科技提醒大家,安裝更新通知請睜大眼:保持作業系統及應用程式更新可防漏洞攻擊,但別更新到勒索病毒!

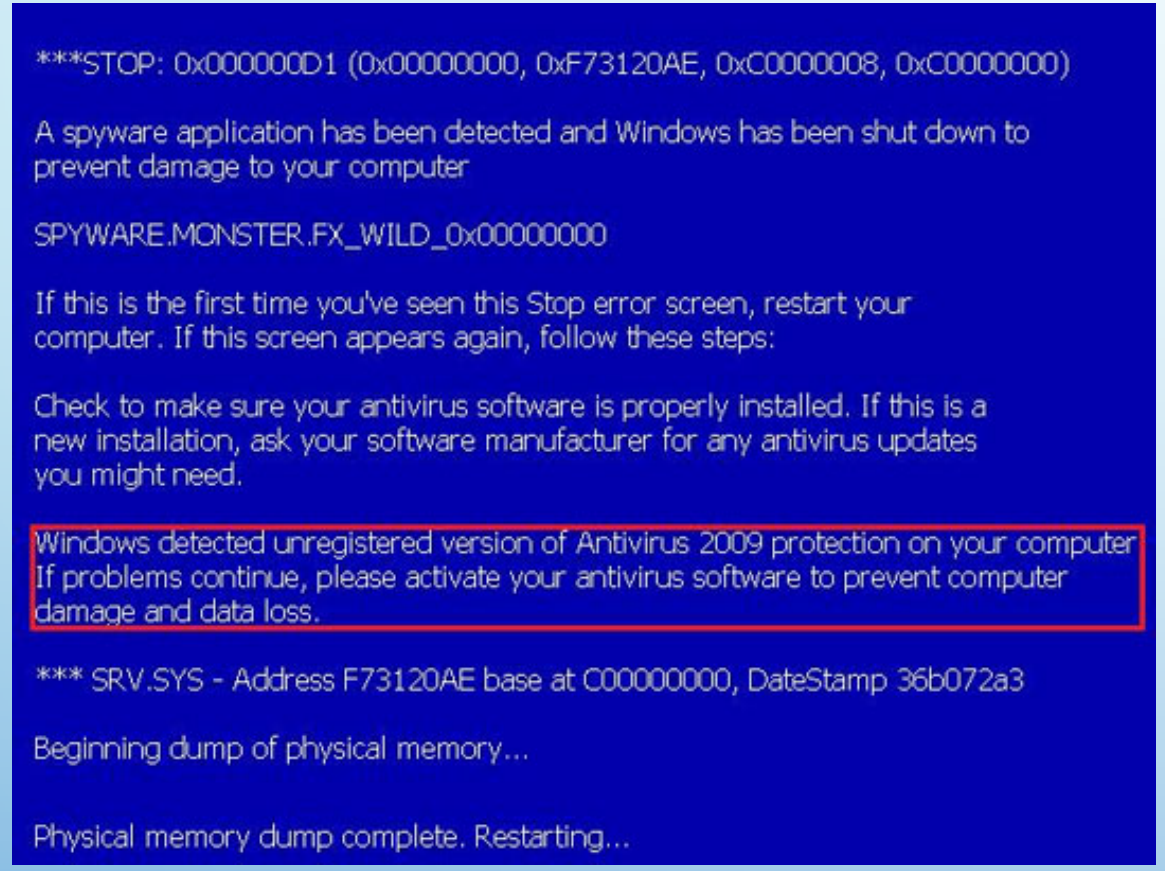
WINDOWS /ADOBE FLASH 更新通知、出現藍屏、網頁變亂碼、假技術支援真詐騙....駭客裝神弄鬼常見 6 招

1. 出現黑畫面,跳出電腦中毒警告訊息
2. 出現亂碼,跳出”找不到字形”對話框;警告必須立即升級
3. 跳出”WINDOWS 或 ADOBE FLASH 更新通知”對話框
4. 出現訊息:「WINDOWS 出現重大問題。千萬別重新開機。立刻跟我們聯絡！」
5. 手機跳出「你感染病毒導致電池損壞」
6. 「恭喜!!!你是今天的幸運用戶，能獲得一台蘋果IPHONE...」

假防毒軟體裝神弄鬼, 新北市王同學付費解毒愈解愈毒(認識假防毒軟體 FAKE AV)

- 2013 年刑事局接獲報案得知，新北市王姓女研究生（廿四歲）點擊網路釣魚（PHISHING）的連結，隨即出現即時掃毒畫面的方式，緊接呈現掃毒結果，跑出十餘筆病毒資料，詳細記錄被感染的電腦位置。她多次重新開機，不是顯示微軟開機的黑畫面，就是藍底白字的英文說明，指電腦中毒無法正常運作，必須更新防毒軟體。誘騙王同學線上刷卡。被害王同學付費兩千元後收到「防毒軟體」，結果非但不解毒，反而讓電腦中毒,不僅詐騙刷卡費用，也盜取個人資料。
- 編按:其實這些畫面可能是螢幕保護程式,請參考:當機又重開機！原來是流氓軟體利用螢幕保護程式製造恐慌)

進化版能測知目標電腦上執行的作業系統版本，然後跟著調整相對應的詐騙介面。

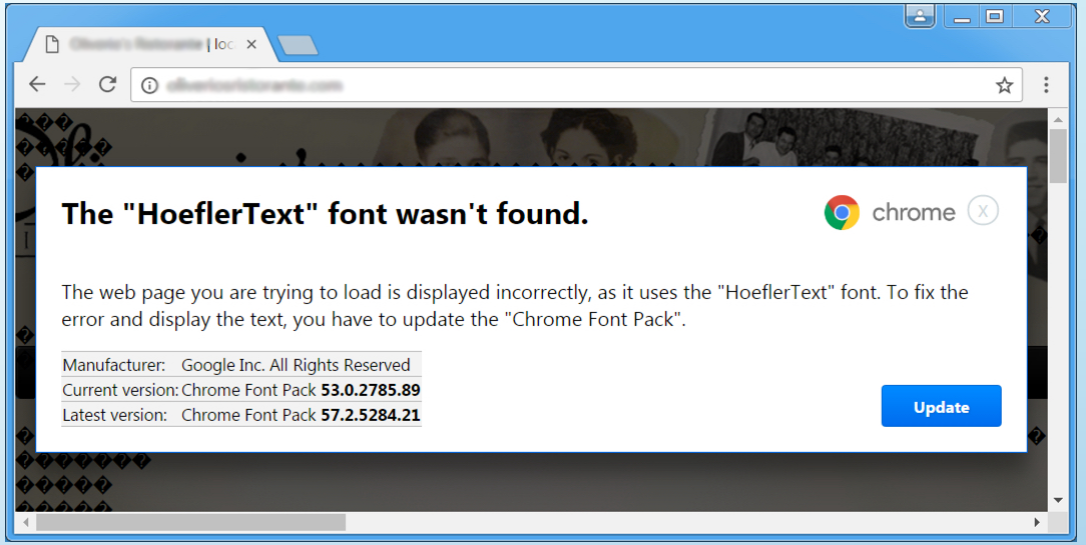


當機與重新開機假畫面其實是螢幕保護程式

- 其實這招勒索病毒也常用,而且還會搬出警察大人嚇唬大家:警察勒索軟體謊稱與防毒廠商簽署國際條約,惡意鎖定受害者電腦勒索贖金,另一個案例是警方:你因觸犯法規電腦遭鎖定，必須支付罰款才能解除鎖定

CHROME 彈出「找不到字型」視窗,別急著按更新,勒索病毒假冒的！

- 之前本落格有提醒大家CHROME 彈出「找不到字型」視窗,別急著按更新,勒索病毒假冒的！



佯稱請使用者更新 Chrome 字型套件的彈出視窗

勒索病毒跳出 WINDOWS 升級視窗,按下 OK,檔案被加密,副檔名還顯示髒話

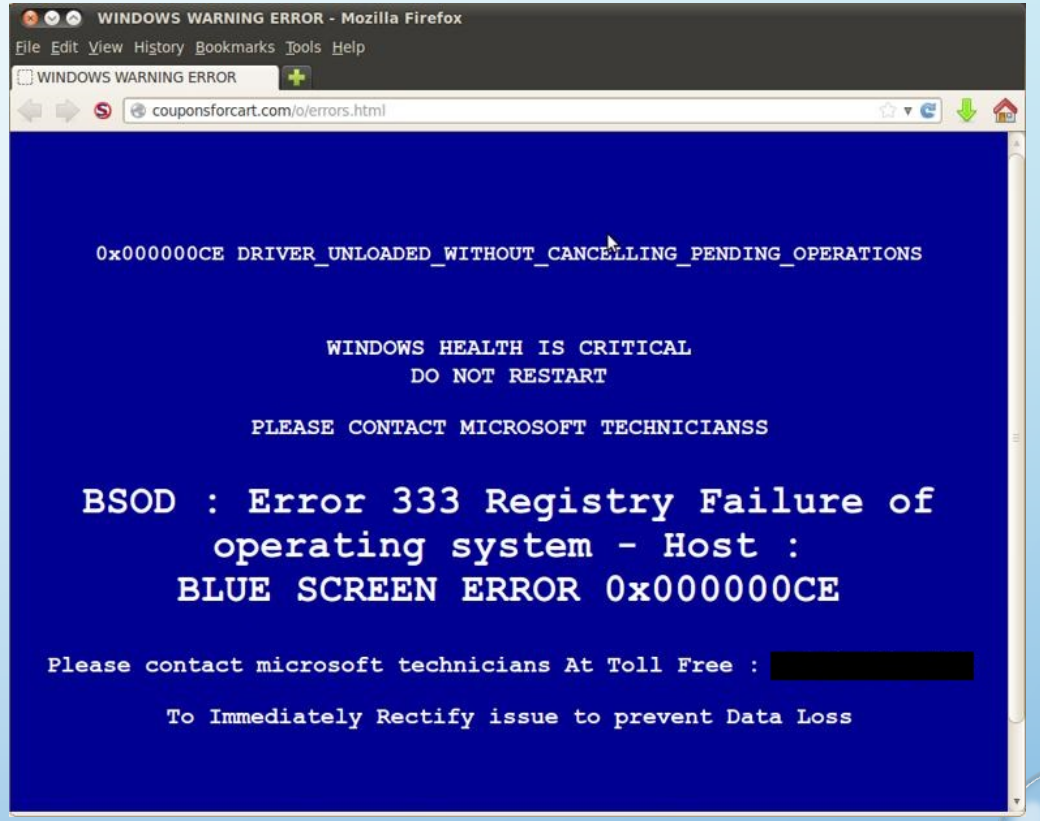
- 另一隻 GC47 (RANSOM_HIDDENTEARGCFS.A)病毒有異曲同工之妙,它會顯示一個假的 WINDOWS 升級視窗來誘騙使用者下載惡意程式。

手電筒應用程式顯示:”你感染病毒導致電池損壞”是惡意廣告

- 並非所有 ANDROID 手機的作業系統都內建手電筒功能。有時候，使用者必須自行下載手電筒程式到手機上才能擁有此功能。但這類應用程式經常含有廣告，並且會不斷更新。根據趨勢科技研究團隊發現，去年 GOOGLE PLAY商店上出現一個會顯示惡意廣告的手電筒程式，不僅為使用者帶來困擾，更會欺騙使用者說他們的手機感染了病毒。且該程式的下載畫面上可看到已累積了6百萬人次下載，影響者眾。

電腦出現藍屏,竟是假的!! 技術支援詐騙暴增,駭客假協助,真詐財!

- 呼籲受害者立即採取行動，例如：「WINDOWS 出現重大問題,千萬別重新開機,立刻跟我們聯絡！」
- 網路詐騙集團已經學會一件事，給您甜頭比恐嚇您更容易讓您上當。
- 歹徒一改過去的恐嚇伎倆，改以「假裝提供協助」的方式來誘騙受害者。這類詐騙會佯稱受害者的電腦遭駭客入侵，並主動提供服務來協助受害者解決問題。
- 通常都是假裝成大公司,如微軟的技術支援人員，並向受害者索取信用卡卡號與個人資訊。



某個遭到感染的網站所顯示的假警告訊息。

填問卷就有機會獲得最新手機?!

- 詐騙步驟:

1. 瀏覽網頁時，跳出以「問卷調查」為名的彈跳式視窗
2. 只要協助回答幾個簡單問題，有機會得到IPHONE手機
3. 問卷最後要求填寫個人資料以進行抽獎，填入EMAIL資料後會自動發送一封確認信，還會給你一組抽獎序號，讓你可以繼續幫忙推廣，甚至宣稱推薦更多人中獎率越高。
4. 這類網站用意是獲得民眾個資後再轉賣，民眾陸續可能會接到一些廣告、行銷、詐騙等電話

遇到彈出警告視窗該怎麼辦?

- 上網時.若瀏覽網頁突然跳出奇怪的視窗或畫面，無論是恐嚇中毒或是恭喜你得獎,請先不要過於驚慌/驚喜。
- 趨勢科技資深技術顧問簡勝財建議:
  - 「馬上將網頁或瀏覽器關閉!千萬不要亂點奇怪的連結或按鈕。
  - 若真的不小心點了，若出現要安裝某某軟體，或是要輸入帳號密碼等個人資訊。請直接關不要安裝或輸入個資。
  - 部分勒索病毒會利用軟體漏洞進行攻擊。因此建議要定期更新軟體修補程式或更新程式，除此之外最好的防護是透過防毒軟體協助攔阻這類攻擊事件。」

6 招防範技術支援詐騙

1. 防範技術支援詐騙最有效的辦法就是**熟知其常用的攻擊伎倆**。
2. 請記住，**真正的技術支援人員不會主動打電話給您**。您必須自己向他們求助。因此，小心那些不請自來的電話。**假若您必須聯絡技術支援人員，請務必確認您手上的電話是對的。請直接前往服務廠商的官方網站來查看他們的支援專線電話號碼。**
3. 若您的螢幕已經被鎖住，然後畫面出現一個惡意廣告，千萬別驚慌。您通常只需**利用 WINDOWS 的「工作管理員」來終止瀏覽器的執行程序即可輕鬆化解**。切記千萬別撥打廣告上的熱線電話。若您在公司裡面，請聯絡您的 IT 部門。
4. 若您聯絡上的支援人員一開始就要求您讓他們**從遠端存取您的電腦**，請提高警覺。遠端存取一般來說都更高階的技術人員才會做的事，而非接電話的第一線人員。
5. 若您已經上當，請盡快採取行動。**若您已經把信用卡資料給了對方，請立刻聯絡您的發卡銀行。若您已經授權給對方進行遠端存取，請馬上變更您的電腦登入密碼。**
6. **安裝一套有效且正派的防毒軟體來避免系統連上惡意網站**。若您已經安裝，切記隨時**保持防毒軟體更新**。唯有保持更新，才能讓您的軟體具備最完整的防護來防範最新的惡意網站。

資料來源

- WANACRYPT0R 2.0 攻擊系統漏洞　台灣成全球第二大勒索病毒受災國家(2017/05/12)。電腦王阿達。HTTPS://WWW.KOCPC.COM.TW/ARCHIVES/146227。
- KPC電腦工作室。(2017/05/13)HTTPS://WWW.FACEBOOK.COM/KPCSTUDIO/POSTS/1371754486226122。
- WANACRYPT0R 2.0 修補 方式全整理　全球災情慘重不要鐵齒(2017/05/13)。電腦王阿達。HTTPS://WWW.KOCPC.COM.TW/ARCHIVES/146257 。
- “ADOBE FLASH 版本太舊需要更新?”按下後卻中了勒索病毒▸遠離 6 種更新通知陷阱(2017/04/25)。趨勢科技。HTTPS://BLOG.TRENDMICRO.COM.TW/?P=49276。