極　機　密
Restricted & Confidential

FAR EASTONE
遠傳

Mobile · Broadband · Media · International Service

新北市政府教育局
資訊安全整合防護委外服務計畫

教育訓練簡報
(防毒服務)

講師:李子名
2016.08.18

趨勢科技防毒服務

摘要

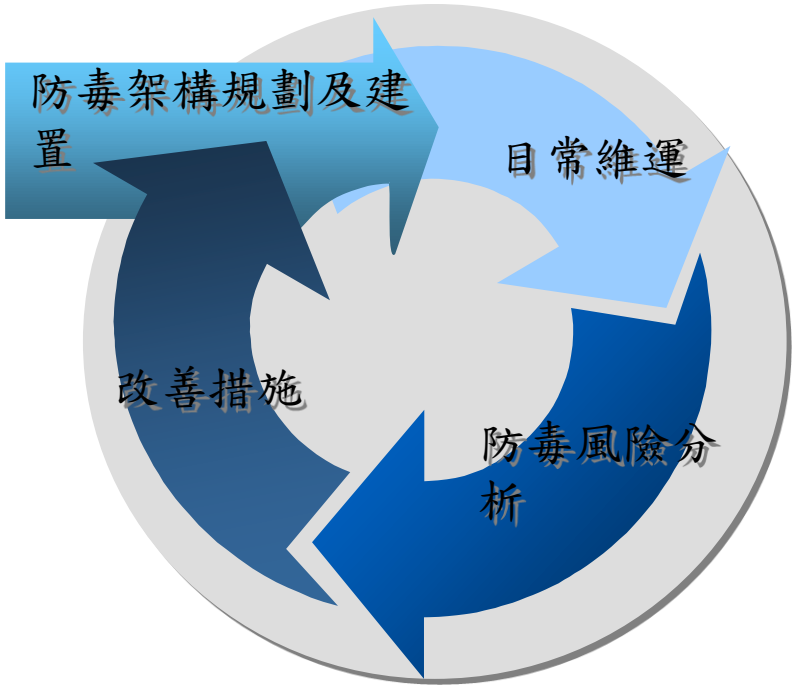
- ESO 服務說明
  - 服務說明
  - 介面總覽
  - 病毒處理流程總覽
  - 病毒處理流程細項介紹
  - 用戶端安裝流程與注意事項
  - SOC 入口網站可以查詢到病毒資訊
- 勒索軟體與行動裝置防護
  - 勒索軟體介紹與防護與解密工具
  - 行動裝置防護
- OSCE11用戶端新功能介紹

ESO 服務

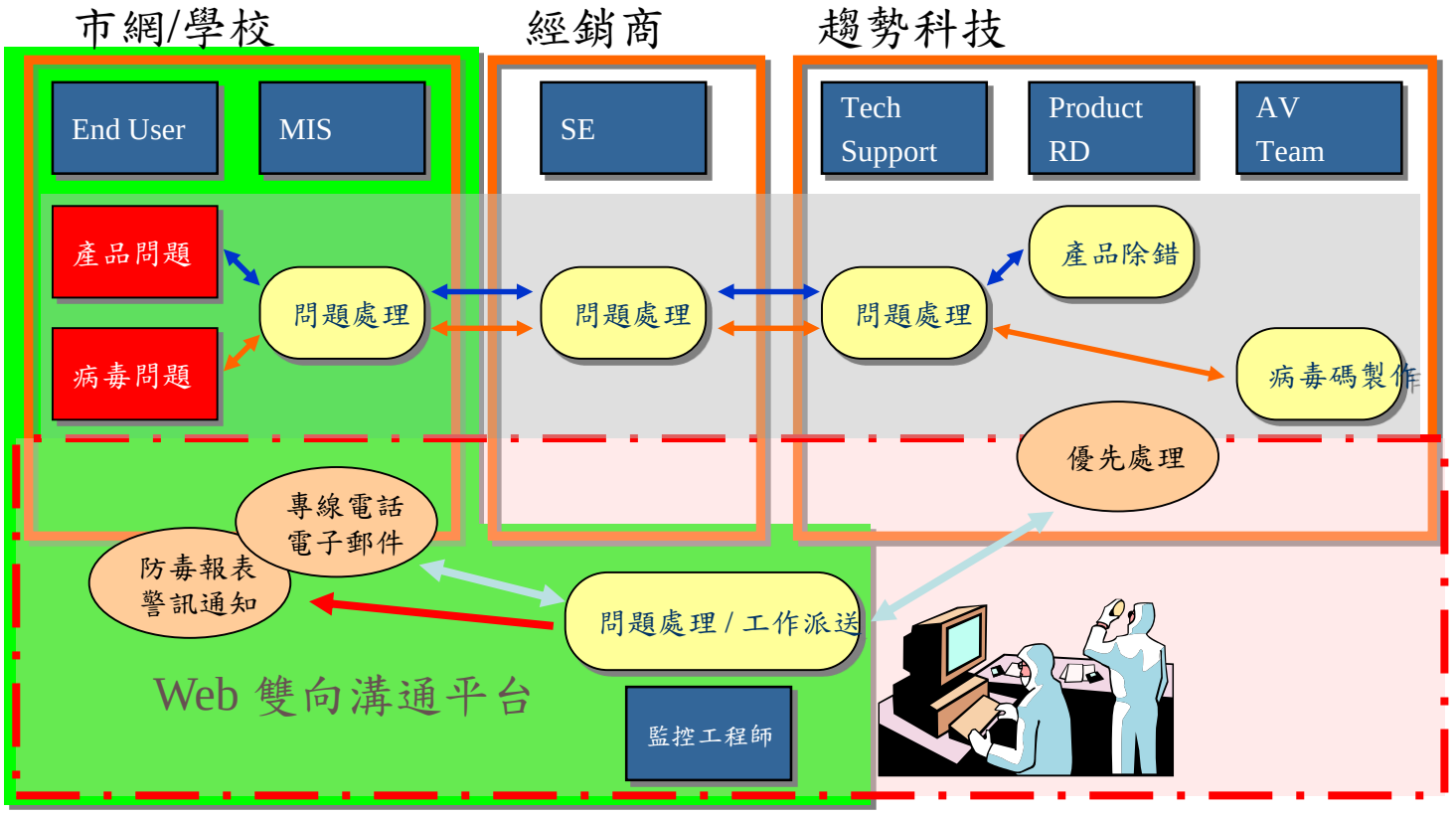
- 服務說明
- 介面總覽
- 病毒處理流程總覽
- 病毒處理流程細項介紹
- 其他說明

服務說明

- 專屬惡意程式清除工具
- 專屬案件管理系統
- 專屬技術支援



專屬技術支援

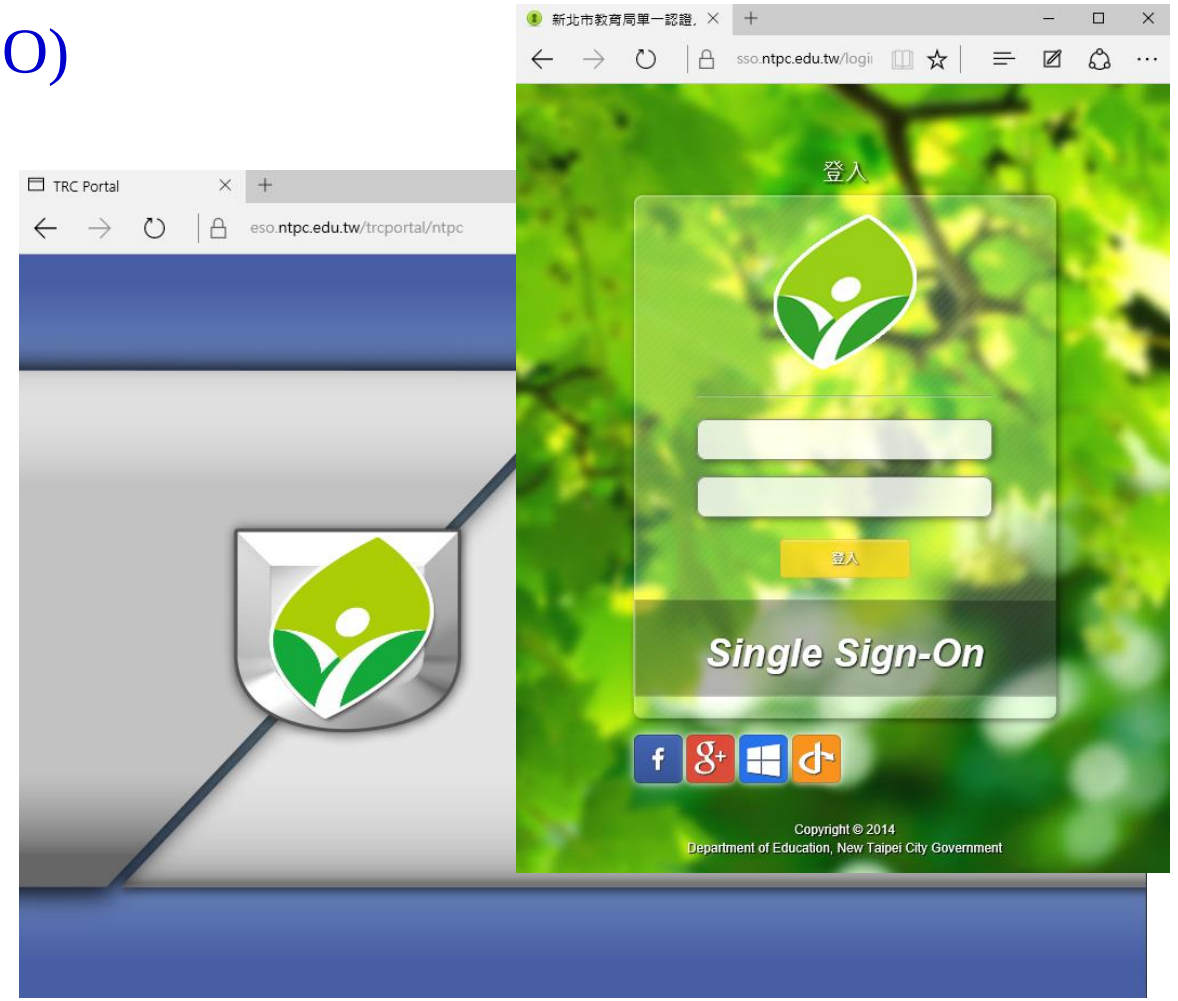


ESO 監控中心

服務說明

https://eso.ntpc.edu.tw (支援SSO)

- 客製化清除工具
- 提供多管道諮詢平台
- 病毒處理程序簡化
- 快速的回應機制
- 提升服務品質



介面總覽

❑ 摘要


首頁
諮詢服務
監控資訊
報表
技術支援
客戶專屬
使用說明
管理
最新惡意程式
最新垃圾郵件
最新惡意URL
最新安全弱點
偵測名稱 公告日期 整體風險分級 病毒碼版本
RANSOM_MADLOCKER.B 09 二月 2016 低 12.319.00
TROJ_KILLDISK.C 28 一月 2016 低 12.257.00
RTKT_BLACKEN.C 28 一月 2016 低 將於近期提供
BKDR_BLACKEN.B 28 一月 2016 低 12.255.00
RANSOM_MEMEKAP.A 26 一月 2016 高 12.297.00
RANSOM_CRYPTRITU.A 05 一月 2016 高 將於近期提供
RANSOM_CRYPTESLA.YYSIX 08 十二月 2015 高 12.199.00
RANSOM_CRYPCHIM.A 03 十二月 2015 高 將於近期提供
TSPY_DRIDEX.YJL 25 十一月 2015 低 12.159.00
TSPY_DRIDEX.SPB 25 十一月 2015 低 12.159.00
更多資訊...
最新問題
熱門問題
常見問題
諮詢百科
1 Deep Security Notifier的資源利用可能會導致系統不穩定
2 使用Internet Explorer時，URL過濾功能無法阻擋"HTTPS"傳輸。
3 使用 IE InPrivate 瀏覽無法無法阻擋封鎖HTTPS流量
4 OfficeScan 10.5 與 10.6 周邊設備存取控管的USB權限有何不同。
5 Control Manager（TMCM）是否支援 Microsoft SQL Server 2012？
6 如何升級角色分別為 Parent 與 Child 的 Control Manager（TMCM）6.0 伺服器？
7 在安裝 SQL Server 期間連線到自訂的通訊埠
8 比較OfficeScan 8.0 和 10.6的系統需求及產品功能
9 當 OfficeScan 行為監控驅動程式嘗試檢索完整路徑名稱時發生 BSOD 的狀況。
10 如何從 Linux 上移除 Deep Security Agent (DSA)

案件管理系統(各校有專屬登入帳號)

防毒相關工具(T-Clean) 下載

T-Clean

工具說明

主要功能

- 有效清除近期台灣地區常見的變種病毒、木馬及惡意程式。
- 防止持續變種的惡意程式再次寫入電腦系統中。
- 可收集可疑檔案、系統相關資訊及趨勢科技防毒軟體病毒記錄檔，並可回傳趨勢科技技術服務中心作進一步分析。

T-Clean並非是使用防毒軟體的病毒碼，而是針對常見的惡意程式檔案機碼進行刪除及運用新功能TDME追蹤重點檔案的關聯程序及追蹤重點惡意DNS 查詢關聯，並刪除。

重要:T-clean不定時更新並放到下載路徑，需要才下載！

學校端防毒管理步驟

1. 處理學校用戶端需求

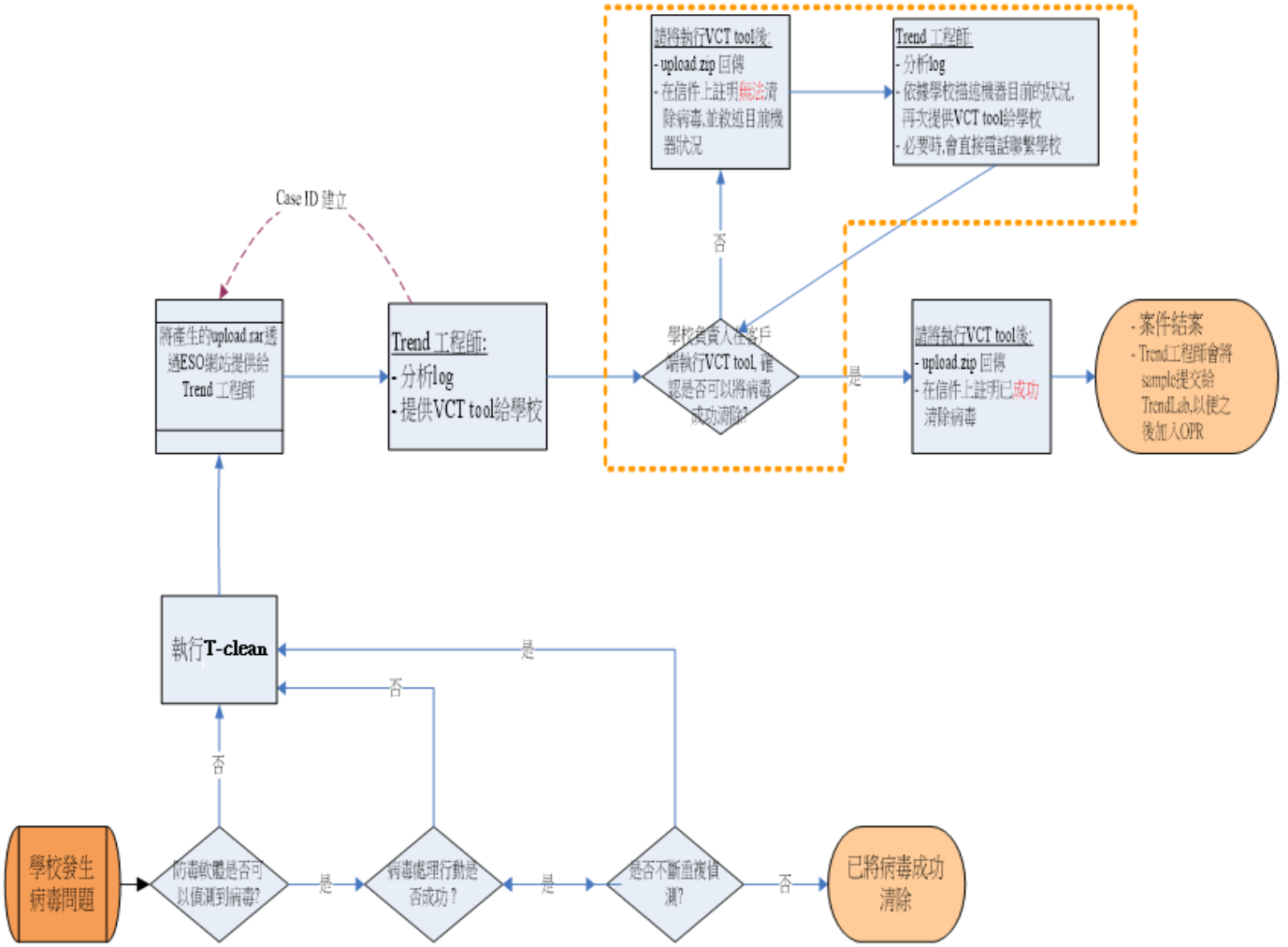
- 疑似中毒、暫時無法偵測之病毒(從防毒管理系統下載並執行T-Clean)
- 將收集的病毒樣本回傳至趨勢科技分析，趨勢將會給予一個客製化的清除工具

2. 學校應了解自身狀況

- 分析感染原因：外來電腦、漏洞未補、未設密碼、上不良網站...
- 分析感染管道
- 制定學校安全政策、加強防禦、教育訓練

P.S. 合約內提供**無限次數專線電話支援**與防毒管理系統之線上諮詢服務。

病毒處理流程總覽



病毒處理流程細項介紹 – 判定是否需要執行清除工具(1)

病毒處理步驟:

步驟1. 學校反應病毒問題

→ 趨勢客服會協助確認病毒問題

步驟2. 客服會確認是否趨勢的防毒軟體可以偵測到？

- 是: 請執行步驟3
- 否: 請執行步驟6

步驟3. 客服會確認毒軟體執行病毒處理行動是否成功?

- 是: 請執行步驟4
- 否: 請執行步驟6

病毒submit流程細項介紹 – 判定是否需要執行清除工具(2)

步驟4. 防毒軟體是否一直重複偵測到病毒?

- 是: 請執行步驟6

- 否: 請執行步驟5

步驟5. 請與客戶說明, 趨勢防毒軟體已將病毒成功清除

========== 結束 ==========

病毒處理流程細項介紹－如何使用執行工具(1)

步驟6. 請到ESO網站-**客戶專屬**>下載T-Clean

https://trc.trendmicro.com.tw/TRCPortal/TClean/DownloadFile

依照下列步驟執行此工具:

PS. 此工具會不定期更新, 建議每次到客戶端之前, 可以先行下載當時最新版本!!

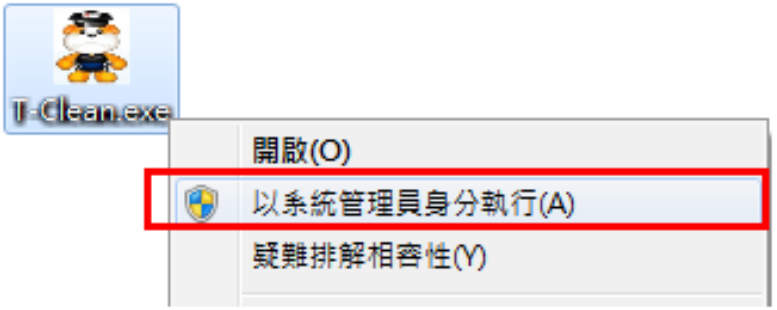
(1) 解壓縮下載的壓縮檔 (解壓縮密碼:novirus)

(2) 使用滑鼠點兩下T-Clean.exe ,程式會開始收集病毒相關資訊,執行收集資訊期間會出現以下視窗, **請勿**將其關閉

T-Clean
執行步驟

1.將下載完成的T-Clean.zip解壓縮，解壓縮密碼為 novirus。

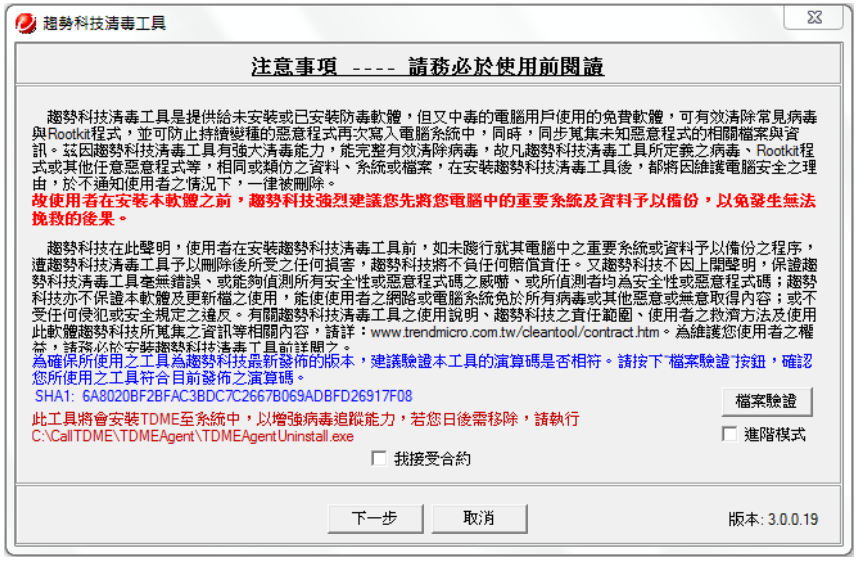
2. 請點選執行T-Clean.exe，若為Vista、Windows 7、Windows 2008，請於T-Clean.exe點選滑鼠右鍵，點選以系統管理員身分執行。



T-Clean
執行步驟

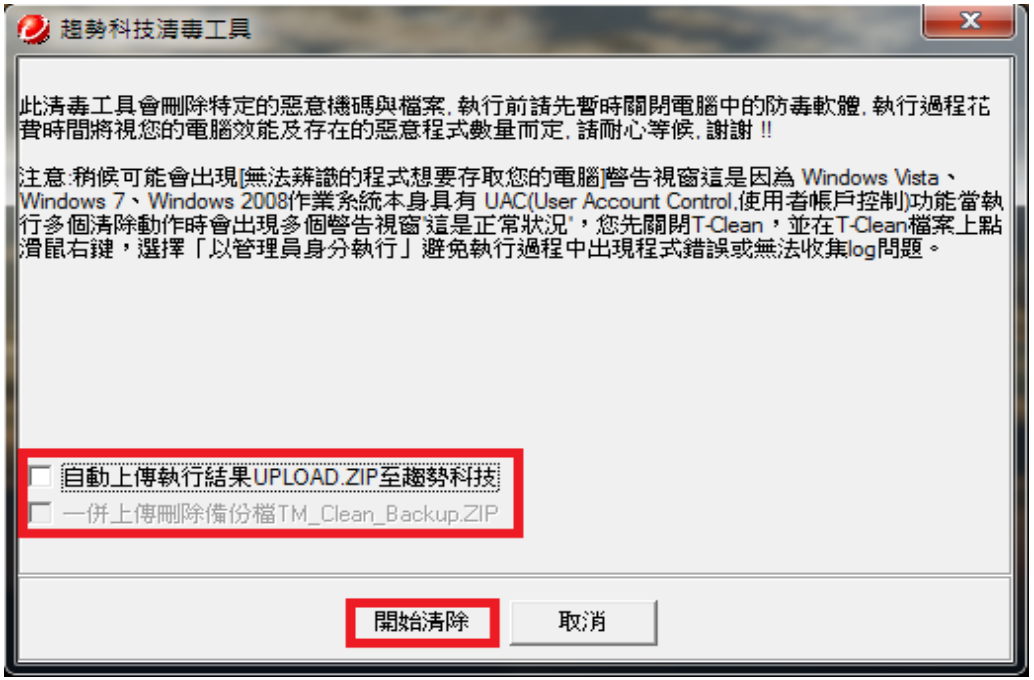
3. 請詳細閱讀授權合約內容，並點選「檔案驗證」，此為確保使用之工具為趨勢科技最新發布的版本，若檔案驗證無誤，會出現檔案SHA1驗證無誤，若出現錯誤，請重新下載最新發布的T-Clean工具。

4. 驗證完成後，請按下「我接受合約」，並點選下一步。



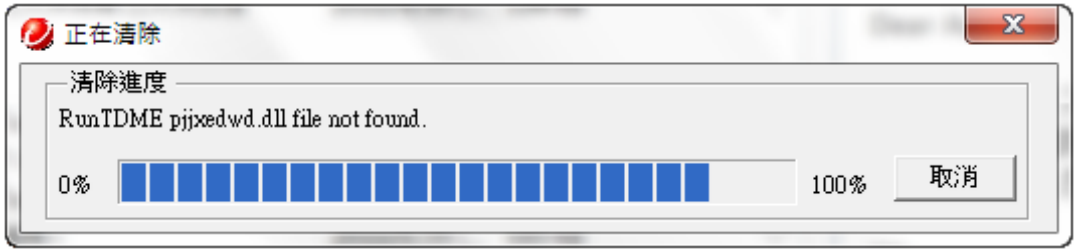
T-Clean執行步驟

4. 請確認相關說明，此工具會暫時關閉電腦中的防毒軟體。取消勾選「自動上傳執行結果UPLOAD.ZIP至趨勢科技」，並點選「開始清除」。



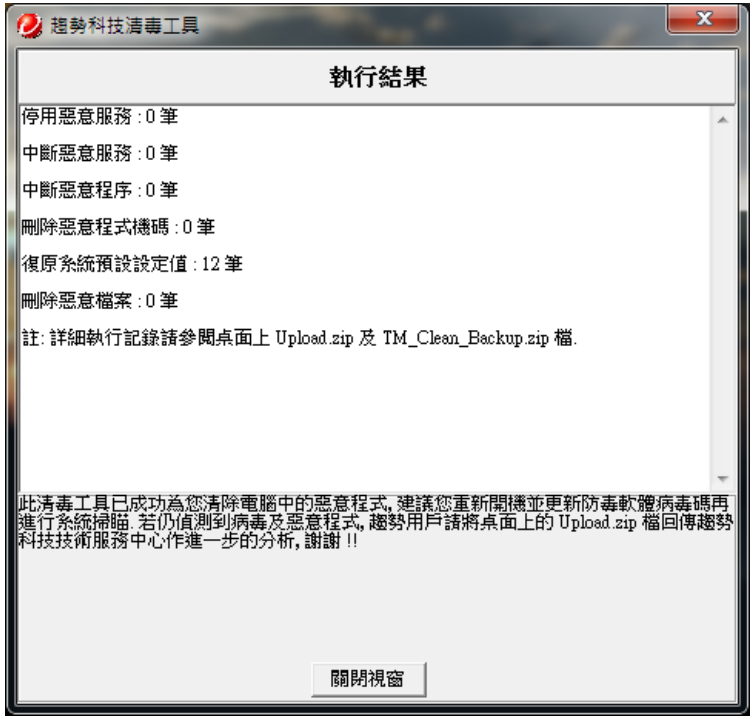
T-Clean
執行步驟

5. 執行所需時間，將視您的電腦效能及存在的惡意程式數量而定，請耐心等候。



T-Clean
執行步驟

6. 當執行完成後，會顯示執行結果，並產生TM_Clean_Backup.zip(已被刪除的惡意檔案相關記錄) 及Upload.zip (執行過程相關記錄)於桌面，請回傳上述檔案，並請點選「關閉視窗」結束T-Clean工具。



病毒處理流程細項介紹 – 如何submit 檔案

步驟7.

7.1 請透過線上處理案件系將upload.zip提交給趨勢科技工程師

請注意: 1. 請務必依照下列註明事項填寫

2. 僅適用於縣網指定的學校提交病毒案件使用

- 部門名稱: 請填寫學校名稱

- 聯絡人姓名/聯絡人電子信箱/聯絡電話: 請填寫負責老師聯絡資訊

E-mail & 電話請務必填寫正確, 以便於之後tool 的提供以及後續的聯絡

- 問題描述: 請儘量寫清楚所遇到的問題,以避免因為資訊不清楚,

造成信件往返多次,延遲病毒分析速度

(請務必依照指定格式填寫)

病毒處理流程細項介紹 – 如何submit 檔案

避免開啟未經確認的電子郵件或者點選郵件當中的連結，這類連結一旦點選就會啟動勒索病毒安裝程序。

備份您的重要檔案，遵守 3-2-1 原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。

定期更新系統、軟體及應用程式，讓您的應用程式隨時保持最新狀態，防堵最新的漏洞。

解密工具說明

http://esupport.trendmicro.com/solution/zh-TW/1114221.aspx

相關資料也可參考TRC Portal → 技術支援 → 技術文件下載 → 勒索病毒相關文件

病毒處理流程細項介紹 – 分析& 提供清除工具

步驟8. 趨勢科技工程師根據學校提供的資訊以及log,

分析後會透過E-mail提供專屬清除工具給學校

病毒處理流程細項介紹 – 分析& 提供VCT工具(2)

步驟9. 學校將取得的清除工具依照下列步驟在用戶端執行,確認是否可以將病毒清除

步驟:

(1) 學校會收到步驟8的信件, 裡面會包含清除工具下載路徑, 請下載此工具

(2) 請在之前收集SIC log 的機器上執行此工具

(3) 執行完畢後,程式會自動在桌面產生Upload.zip (解壓密碼:virus)

(4) 確認是否已將病毒成功清除

- 是: 請執行步驟10
- 否: 請執行步驟12

病毒處理流程細項介紹 – 回報清除狀態&提供Upload.zip - 成功(1)

步驟10. 請將執行完清除工具後產生的Upload.zip

- 使用回覆的方式將Upload.zip 附加於Email 回傳給趨勢科技工程師

PS. 若是Upload.zip檔案太大無法上傳，請與ESO客服人員聯絡

- 並請在信件內文註明已**成功**清除病毒

病毒處理流程細項介紹 – 回報清除狀態&提供Upload.zip - 成功(2)

步驟11. 當趨勢科技工程師收到回覆的信後

- 會將此案件結案

- 將Upload.zip提供給TrendLab, 便於日後加入正式版的病毒碼中

========== 案件結束 ==========

病毒處理流程細項介紹 – 回報清除狀態&提供Upload.zip - 失敗(1)

步驟12. 請將執行完清除工具後產生的Upload.zip

- 使用回覆的方式將Upload.zip 附加於Email 回傳給趨勢科技

  工程師

PS. 若是Upload.zip檔案太大無法上傳，請與ESO客服人員聯絡

- 請在信件內文註明**無法**成功清除病毒, 並簡述目前機器狀況

病毒處理流程細項介紹 – 回報清除狀態&提供sample- 失敗(2)

步驟13. 趨勢科技工程師分析經銷商再次回傳的log, 並依據學校負責人員描述目前機器的狀況,再次提供清除工具,學校負責人員收到 清除工具後, 再回到步驟9依序執行之

技術支援專線及專屬線上服務

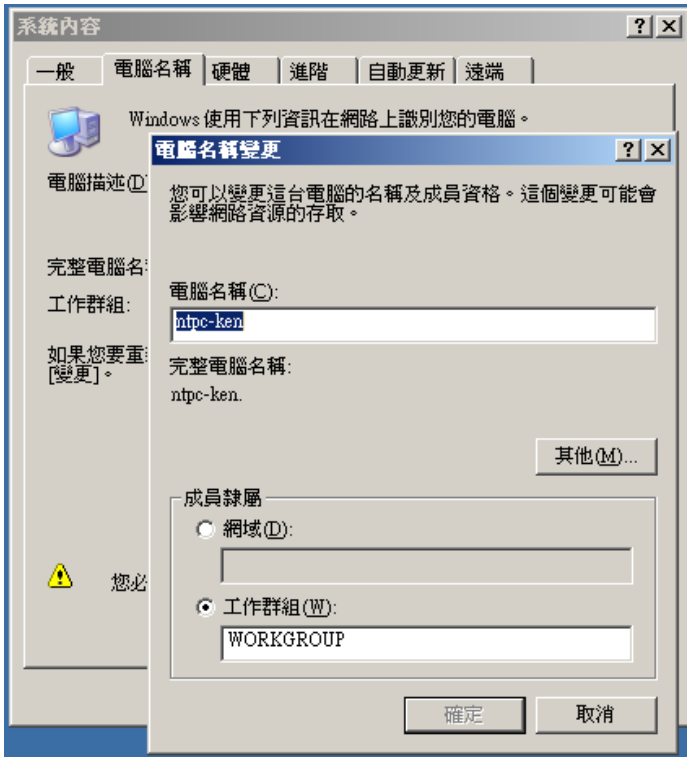
- 技術支援專線: 02-2377-2323#1
- ESO 線上服務申請:https://eso.ntpc.edu.tw

其他說明

Officescan 用戶端安裝

1. 確認電腦的命名規則：

(Domain Name - pc name)

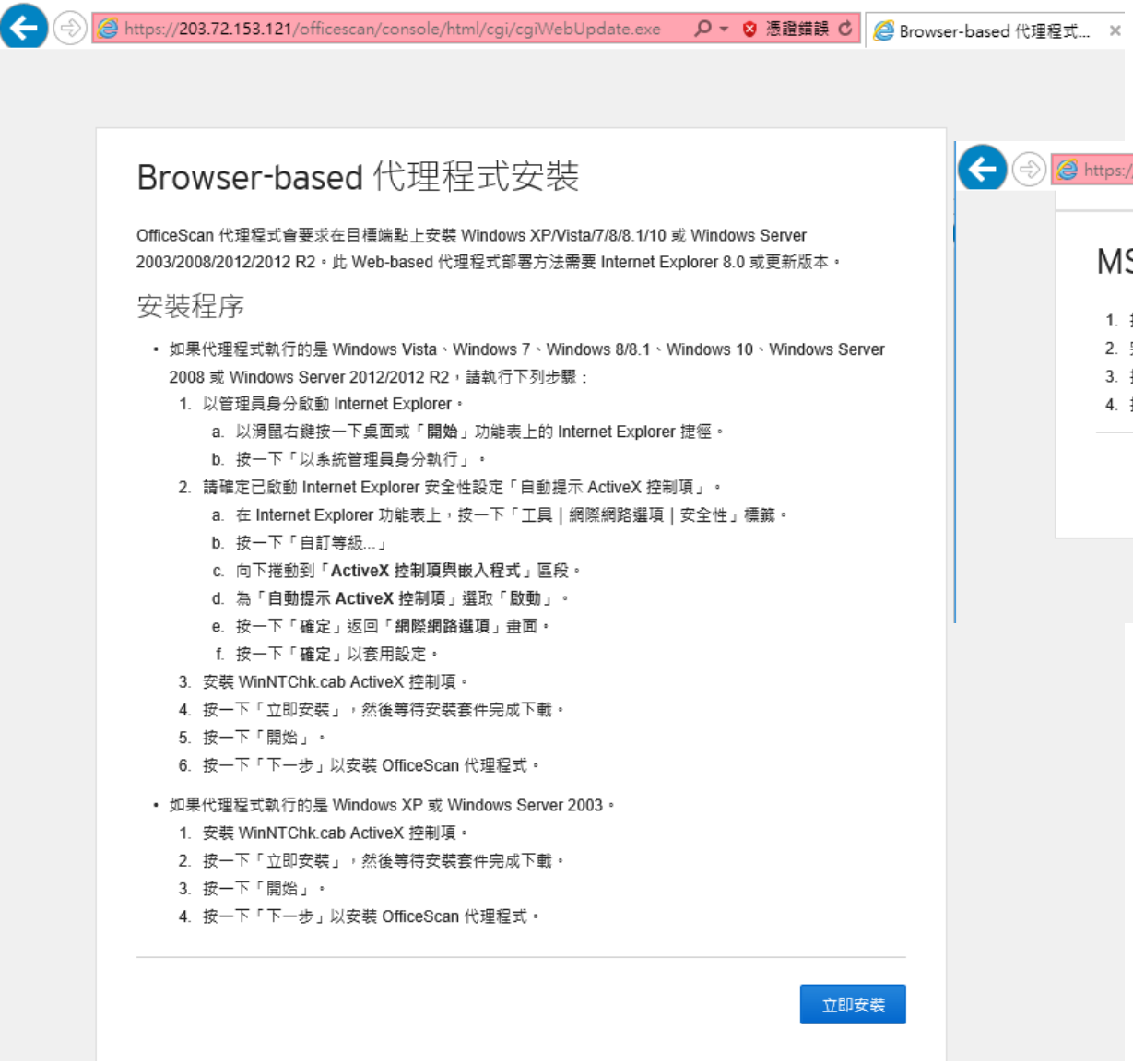


其他說明

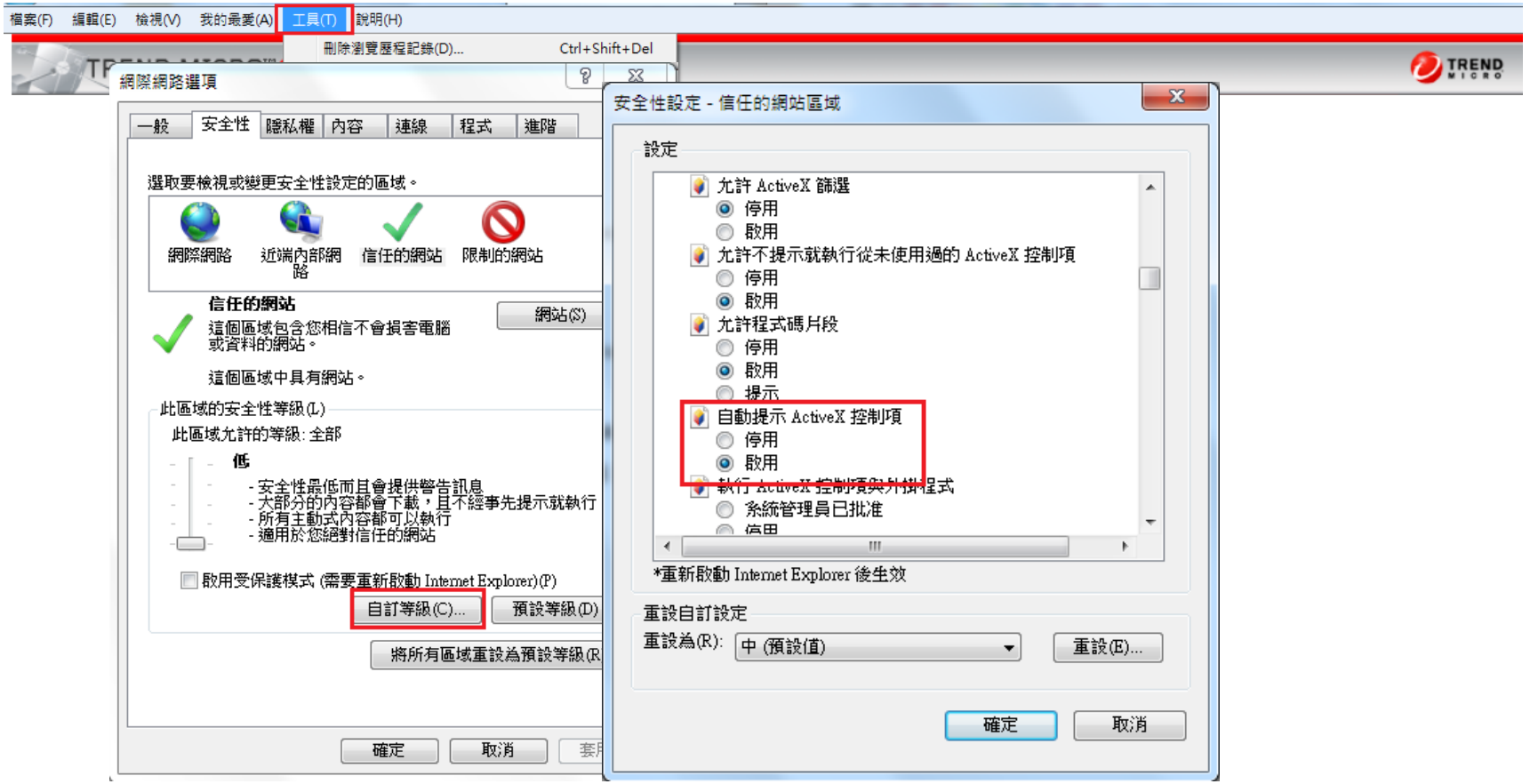
2. 用戶端下載位置

https://203.72.153.121/officescan/console/html/cgi/cgiWebUpdate.exe

OSCE Server(自動轉址連到完整URL)	9大分區學校	29行政區別
203.72.153.121	板橋分區+中心	土城區、板橋區
203.72.153.122	三重分區+三鶯分區	三重區、蘆洲區、三峽區、樹林區、鶯歌區
203.72.153.123	七星分區+新莊分區	汐止區、金山區、萬里區、八里區、五股區、林口區、泰山區、新莊區
203.72.153.124	雙和分區+瑞芳分區+淡水分區+文山分區	石碇區、坪林區、烏來區、深坑區、新店區、三芝區、石門區、淡水區、平溪區、貢寮區、瑞芳區、雙溪區、中和區、永和區

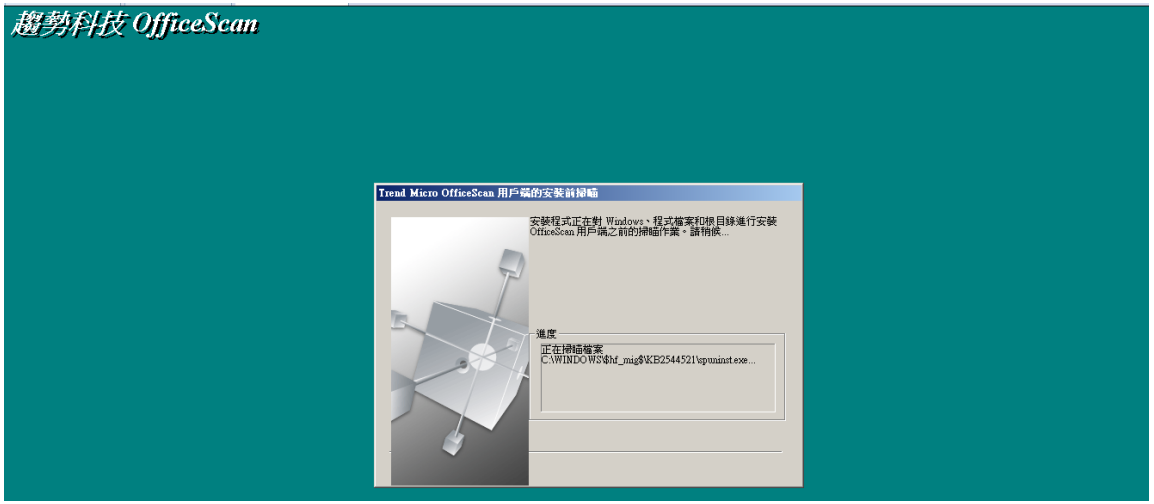


用戶端程式安裝方式-Internal Web Page

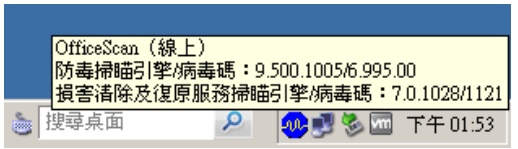


其他說明

3. MSI執行officescan用戶端安裝程式後，程式將自行安裝且連線至教網中心防毒主機



4. 安裝完成確認右下角出現officescan用戶端圖示



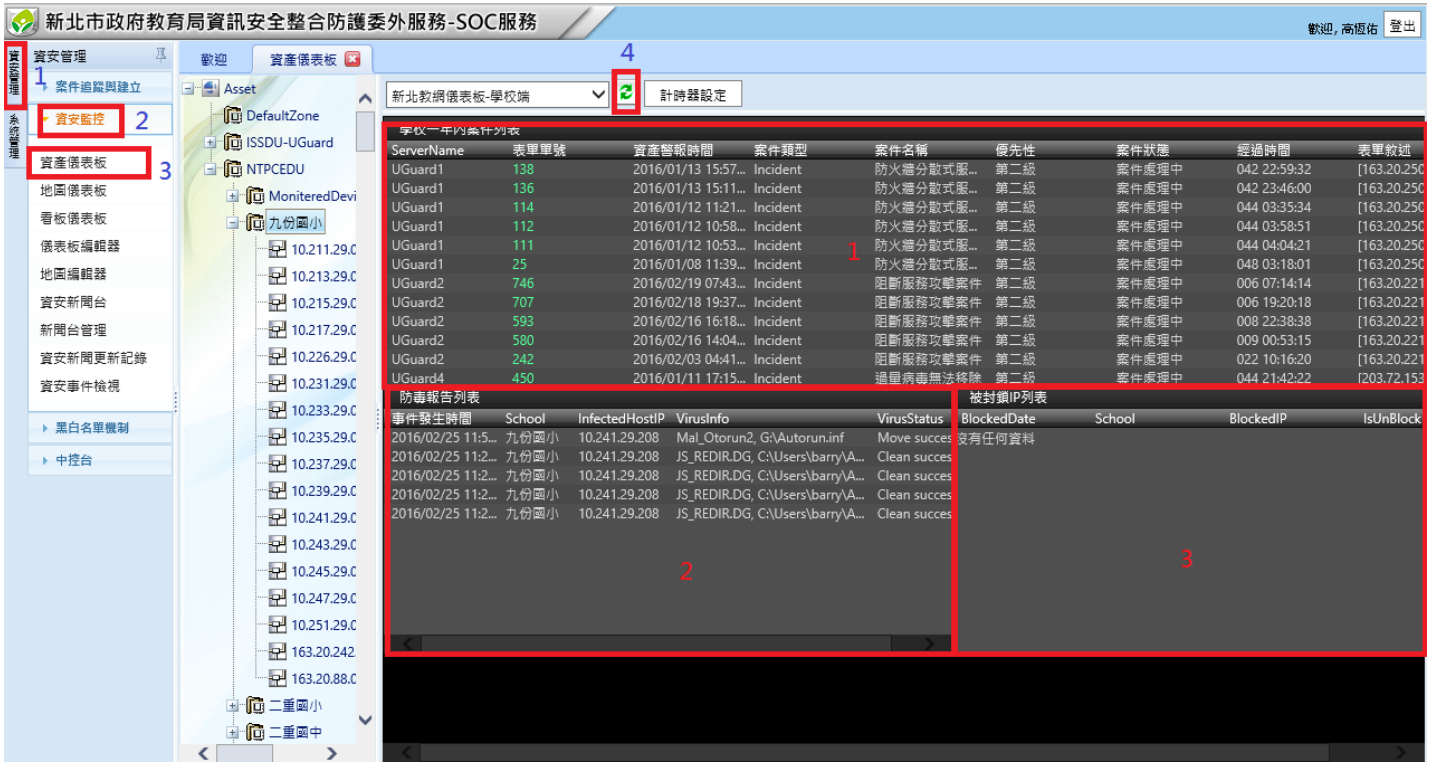
其他說明

4. 如果警告跳出視窗，可以不用立即重新啟動電腦，在方便重啟的時間點進行電腦重新開機即可。

P.S. 若不符合命名原則，而IP又無從判別者，將會被從中控台移除。

UGuard病毒資訊位置查詢

- 登入後-->主選端[資安管理]--->[資安監控]--->[資產儀表板]--->重新整理



極　機　密
Restricted & Confidential

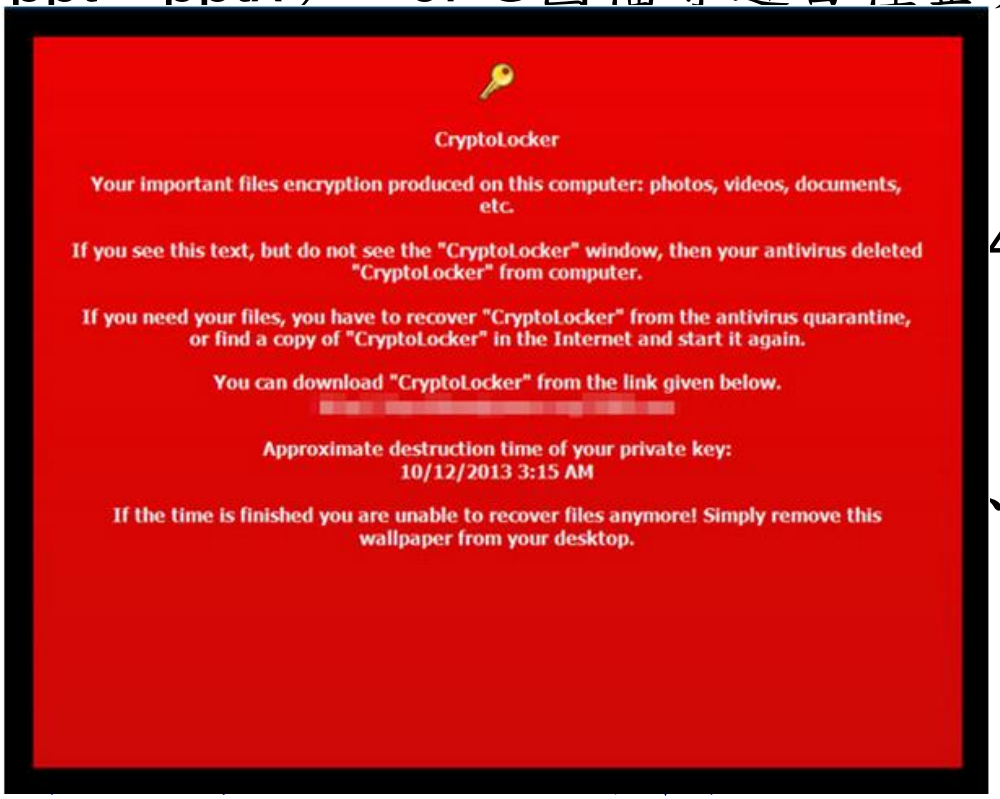
FAR EASTONE
遠傳

Mobile · Broadband · Media · International Service

勒索軟體防護與解密工具

勒索軟體 (Cryptolocker)

- **破壞對象**：電腦內Word（doc、docx）、Excel（xls、xlsx）、PowerPoint（ppt、pptx）、JPG圖檔等近百種企業常見檔案格式。
- 攻擊方式：向遠 48位元RSA和AES加密
- 攻擊範圍：受害 、檔案伺服器等，攻擊公司 置）
- 限制期限內匯款
- 即使發現刪除惡意軟體，文件也無法救回



資安

勒索軟體CryptoLoc

2013年9月初，一隻名為CryptoLoc
現，它會悄悄地將受害者電腦裏的
法破解加密，藉此勒索300美元的

文/ 張景皓 | 2013-11-01 發表

來！開始動手註冊專屬網址　企業體驗4G行動化享好禮　7/3 Akamai Solution Day

新聞

小心！史上最狠毒勒索軟體肆虐臺灣

勒索軟體CryptoLocker大舉入侵臺灣，公司與個人陸續傳出災情，該軟體會將受害者電腦加密，導致檔案無法使用，更限期3天支付9,000元贖金，否則將毀損解密金鑰

文/ 張景皓 | 2013-10-17 發表

按讚加入iThome粉絲團

近日，有一支名為CryptoLocker的勒索軟體（Ransomware）現蹤臺灣，企業陸續傳出受害災情，該軟體透過釣魚郵件入侵，會將受害者電腦的檔案全數加密，導致檔案無法存取，而且駭客採用高超的加密技術，讓受害者無法自行復原，並限期3天支付9,000元贖金，否則將毀損解密金鑰，受害者苦不堪言。

臺灣McAfee技術經理沈志明表示，被加密的檔案，因為私鑰（Private Key）掌握在駭客手裡，基本上使用者不可能自行破解。若是真的要暴力破解，需要運算資源等代價相當高。

CryptoLocker是透過釣魚郵件傳播，使用者若是誤擊

熱門新聞

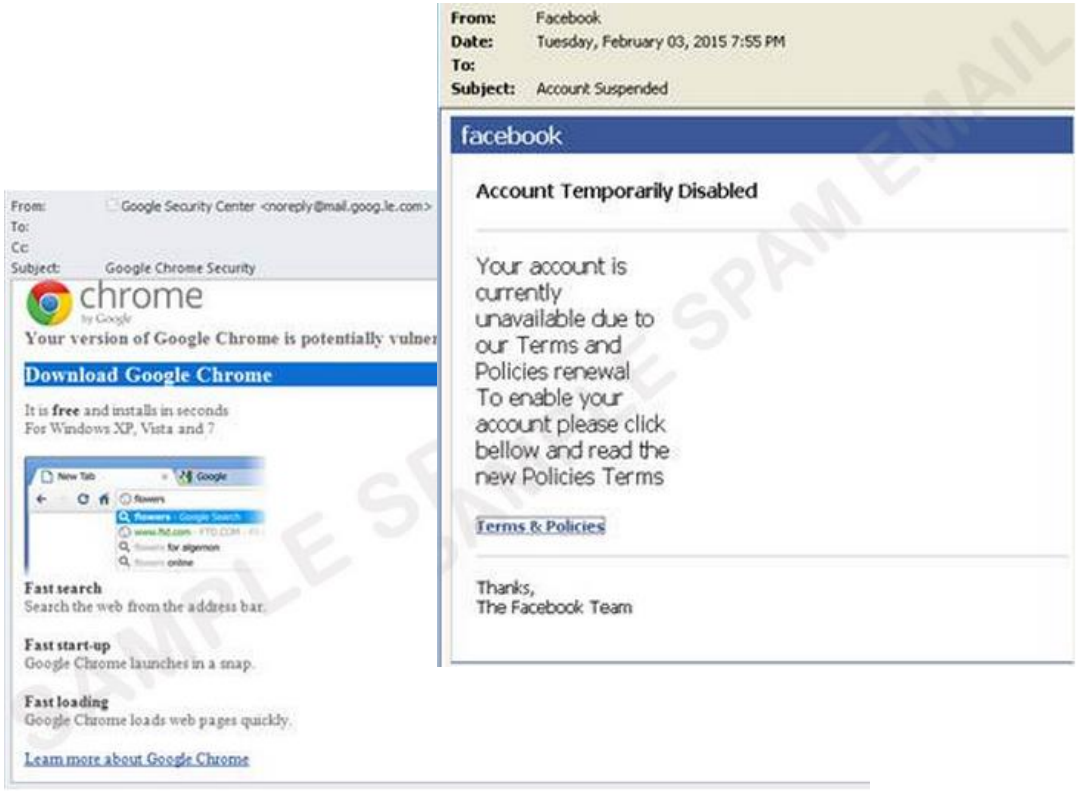

台灣軟體盜版率不降反升，達38%
2014-06-24


Infocus推5吋入門手機M510/511搶攻4G市場
2014-06-24


台灣之星公佈新企業識別，鎖定第三季開通4G服務
2014-06-24

勒索程式假冒 Chrome,Facebook 和 PayPal

- noreply@goog.le.com
- noreply@mail.fb.com
- service@paypal.co.uk



偽裝履歷表壓縮檔

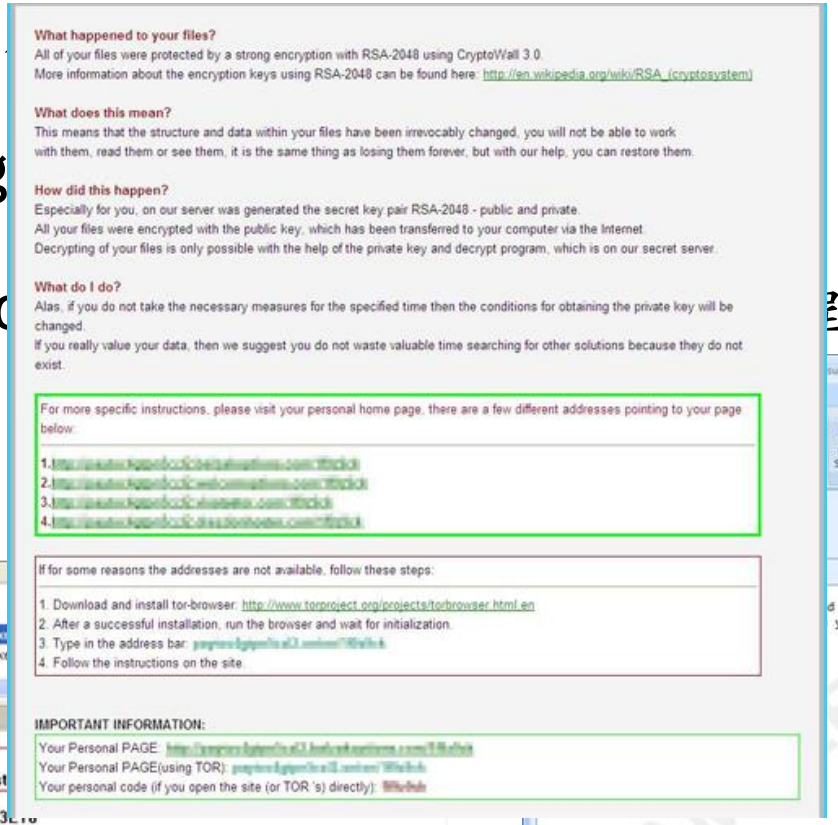
1.社交工程郵件

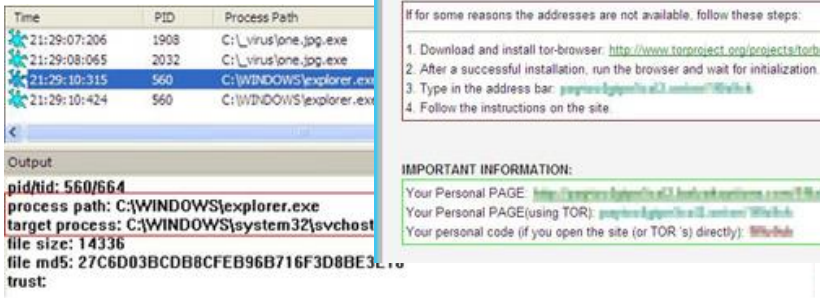
2.解壓縮後檔案

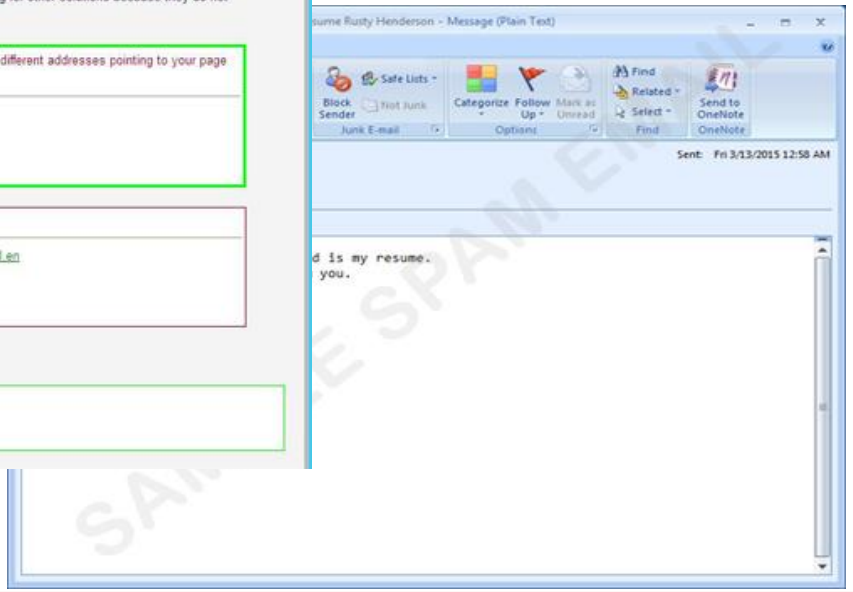
3.上網下載*.jpg

4.偽裝系統explo 程序進行加密

5.彈出綁架訊息







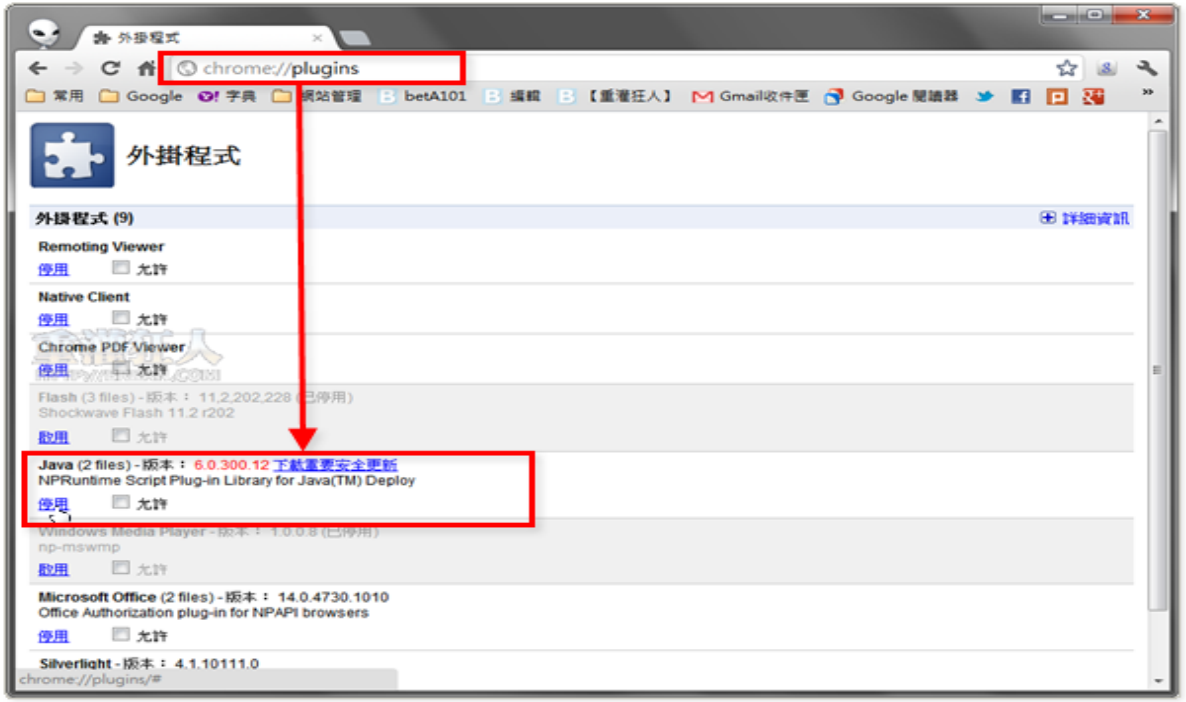
如何預防?

- 微軟系統更新
- 軟體更新(java、flash、office、pdf....)
- 關閉瀏覽器上的 java 、 flash等功能
- 使用者宣導

停用瀏覽器java、flash

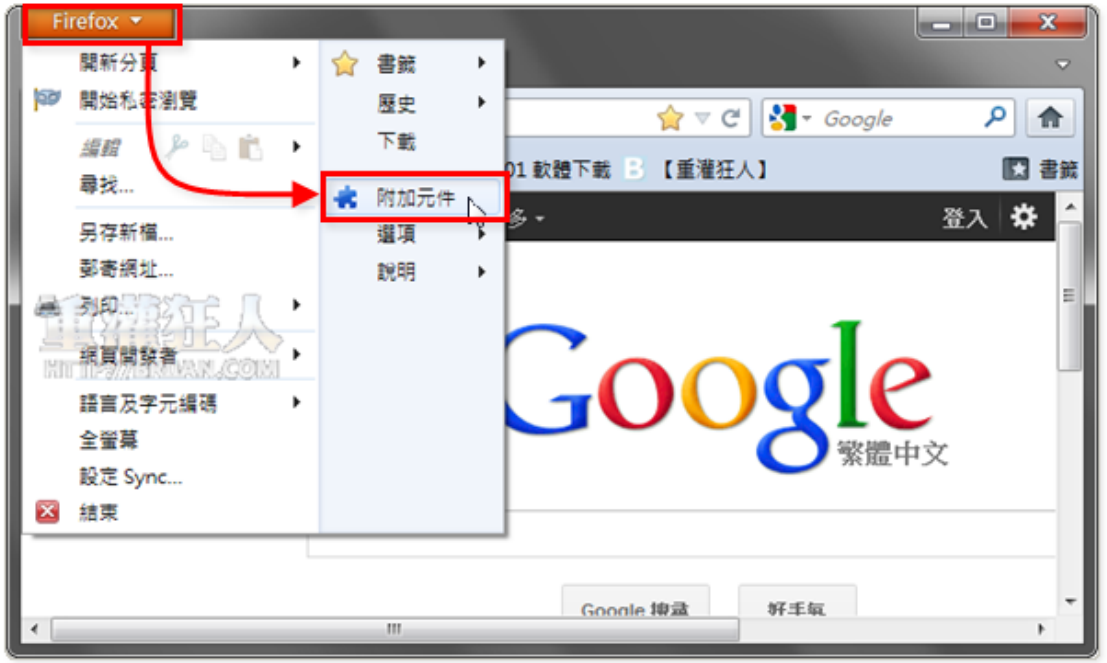
一、在 Google Chrome 中停用 Java、Flash：

第1步 在網址列輸入「**chrome://plugins**」再按「**Enter**」，開啟外掛程式管理頁面後，在你要關閉的項目上按「停用」即可。

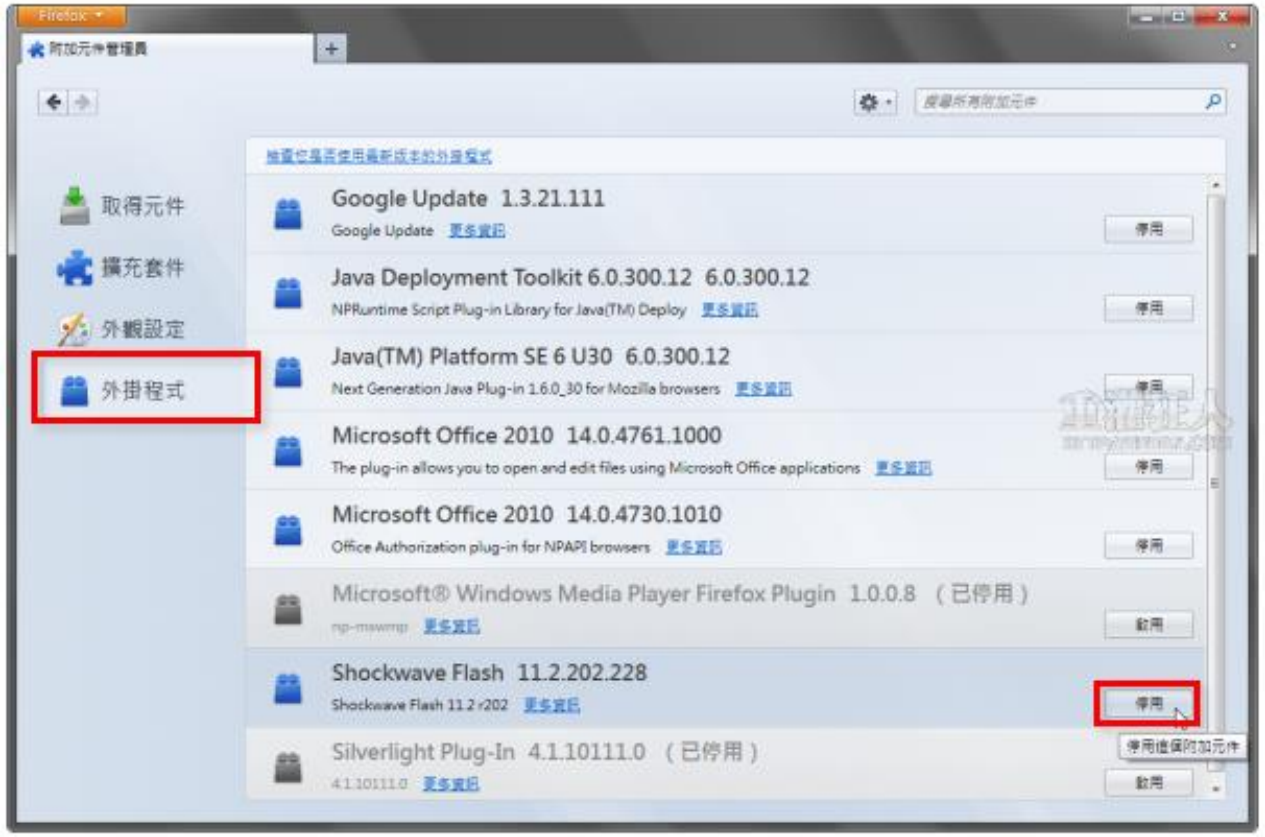


二、在 Firefox 中停用 Java、Flash：

第1步 開啟 Firefox 瀏覽器視窗，按一下左上角的「**Firefox**」選單，點一下「**附加元件**」。



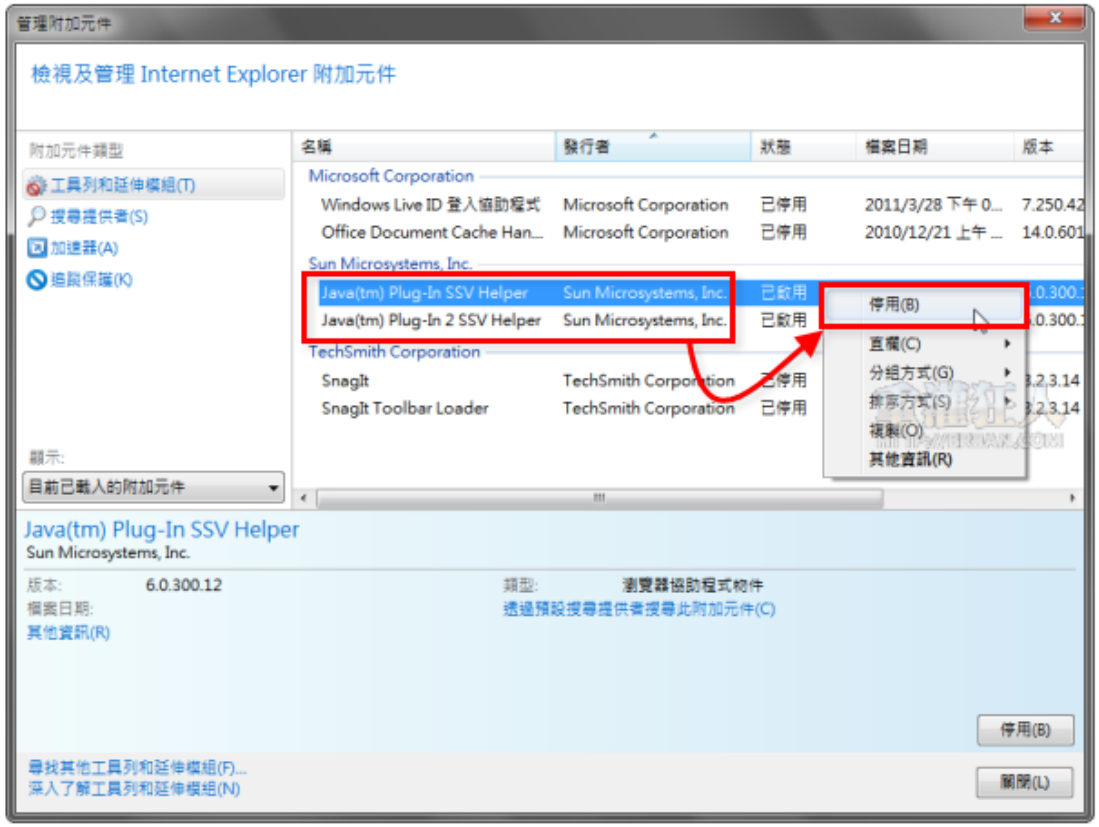
第2步 在「外掛程式」選單中找到你要停用的項目，按一下「停用」即可。



三、在 IE 中停用 Java、Flash：

第1步 開啟 Internet Explorer 瀏覽器視窗，按一下右上角的工具圖示，在選單中點「管理附加元件」。

第2步 在「**工具列和延伸模組**」選單中，找到你要停用的項目再按一下右鍵、點「**停用**」，把你不常用的外掛程式或延伸工具停用，等以後要用時再手動開啟。



被駭後的緊急應變措施

1.立即切斷受駭PC的網路，避免災情擴大

2.更新防毒軟體，清查內網其他電腦，並採取自保措施

3.搶救還沒被加密的檔案

4.若有備份，開始復原檔案

5.評估受害災情，決定是否付贖金取得解密金鑰

6.用新版防毒版本、病毒碼清除，或乾脆重灌電腦

勒索軟體-解密工具

- 支援解密的勒索病毒家族

勒索病毒種類	被加密後的檔案名稱及副檔名格式
CryptXXX V1, V2, V3*	{原始檔案名稱}.crypt 或 crypz 或 5個16進位字元
CryptXXX V4, V5	{MD5雜湊值}.5個16進位字元
TeslaCrypt V1**	{原始檔案名稱}.ECC
TeslaCrypt V2**	{原始檔案名稱}.VVV 或 CCC 或 ZZZ 或 AAA 或 ABC 或 XYZ
TeslaCrypt V3	{原始檔案名稱}.XXX 或 TTT 或 MP3 或 MICRO
TeslaCrypt V4	檔名及副檔名均未被變更
SNSLocker	{原始檔案名稱}.RSNSLocked
AutoLocky	{原始檔案名稱}.locky
BadBlock	{原始檔案名稱}
777	{原始檔案名稱}.777
XORIST	{原始檔案名稱}.xorist 或 隨機副檔名
XORBAT	{原始檔案名稱}.crypted
CERBER	{10個隨機字元}.cerber

勒索軟體-解密工具

注意事項：

- 被 CryptXXX V3 加密的檔案，可能無法完整還原成原始檔案(部分解密)。 詳細可參閱 **[關於 CryptXXX V3 重要說明]**
- RansomwareFileDecryptor 1.0.xxxx MUI 僅能解密 TeslaCrypt V3、TeslaCrypt V4，因此若您被加密的類型屬 TeslaCrypt V1、TeslaCrypt V2，請另外下載 TeslacryptDecryptor 1.0.xxxx MUI 解密工具使用。
- 解密前備份；從單一檔案或資料夾開始解密

勒索軟體-解密工具

工具下載：

- 點選 勒索病毒檔案解密工具(RansomwareFileDecryptor) 取得最新版本趨勢科技勒索病毒檔案解密工具。

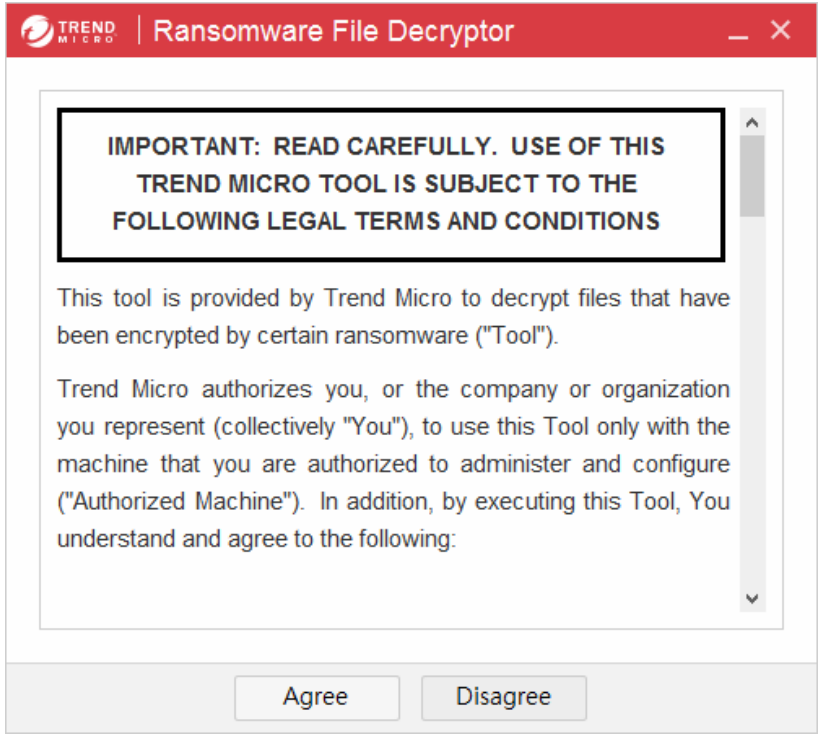
  解壓縮後，請執行其中的 RansomwareFileDecryptor 1.0.xxxx.exe 檔案。

- 點選 TeslaCrypt 解密工具(TeslacryptDecryptor) 取得最新版本趨勢科技勒索病毒檔案解密工具。

  解壓縮後，請執行其中的 TeslacryptDecryptor 1.0.xxxx.exe 檔案。

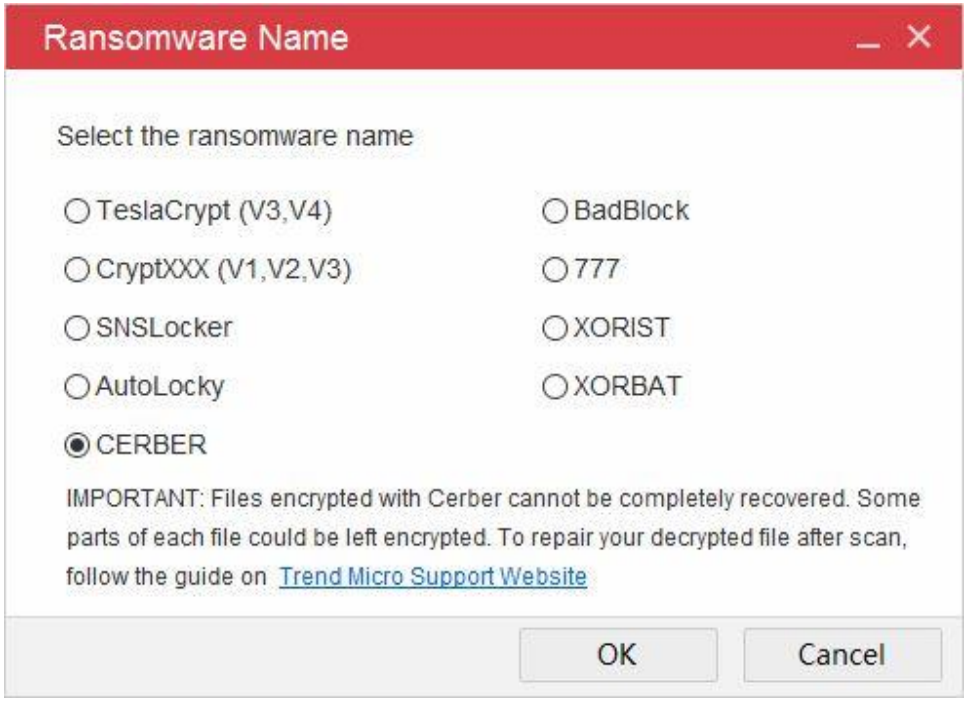
勒索軟體-解密工具

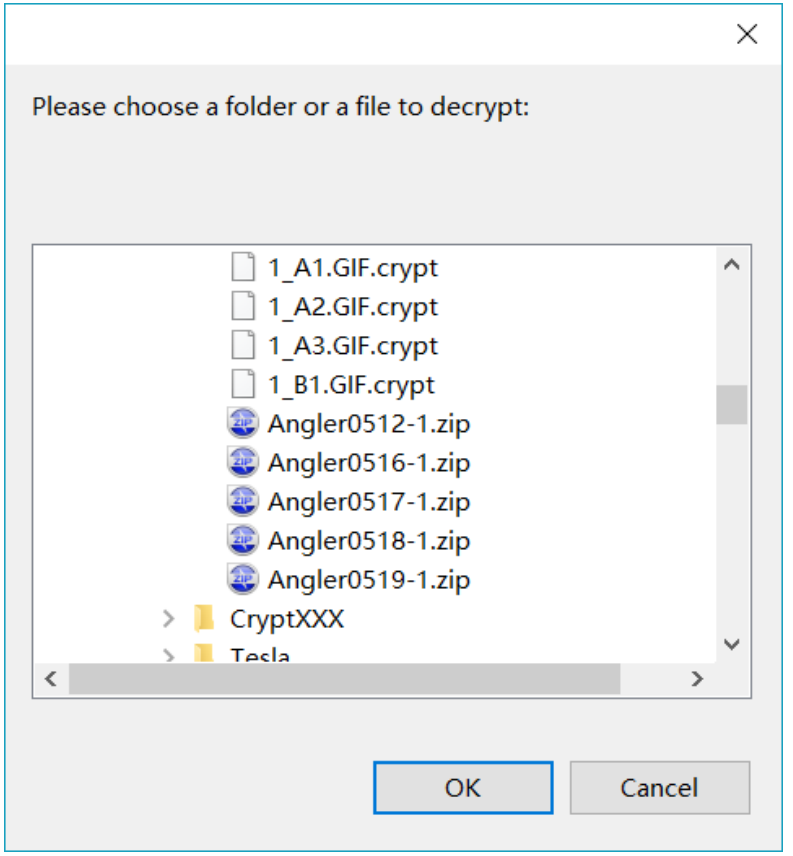
❑ 操作步驟：



勒索軟體-解密工具

- 選擇解密類型與目標





勒索軟體-解密工具

- 檔案解密

勒索軟體-解密工具

- 解密 CyptXXX V1 ， XORIST ， XORBAT需要較多的步驟
- CryptXXX V1 的解密會跳出另一個視窗請使用者協助提供檔案，因此使用者需要分別提供被加密與未被加密檔案各一個。（檔案大小越大越好）

勒索軟體-解密工具

- 完成掃描
- 工具記錄檔%User%\AppData\Local\Temp\TMRDTSelfExtract\LOG
- 工具完整說明http://esupport.trendmicro.com/solution/zh-tw/1114221.aspx

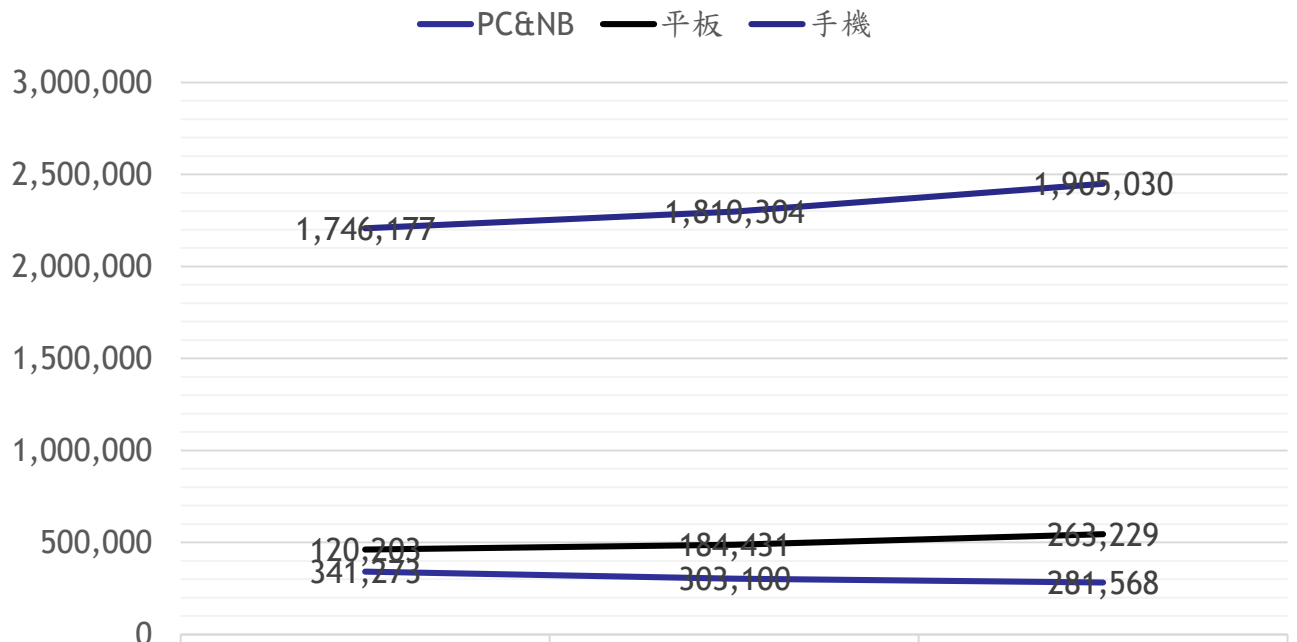
極　機　密
Restricted & Confidential

FAR EASTONE
遠傳

Mobile · Broadband · Media · International Service

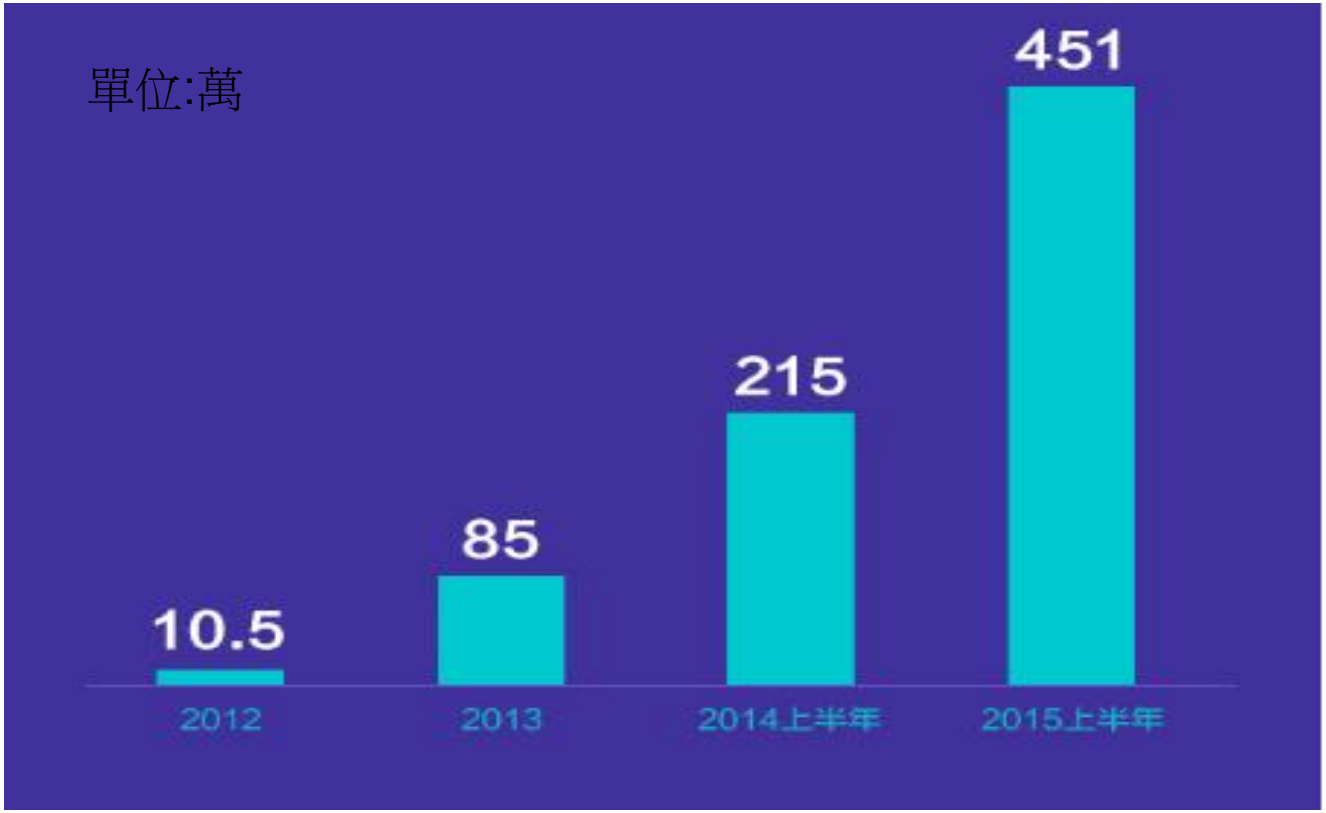
行動裝置(手機、平板)防護

全球裝置出貨量



	2011	2012	2013
手機	1,746,177	1,810,304	1,905,030
平板	120,203	184,431	263,229
PC&NB	341,273	303,100	281,568

手機病毒成長數量

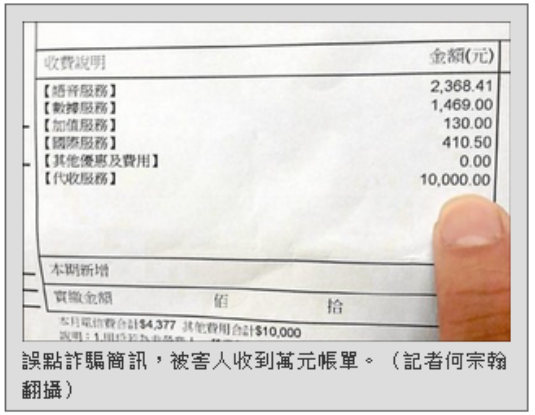


新聞事件

不識詐騙簡訊 連點10次一萬飛了

2014-06-23

〔記者姚岳宏、何宗翰／綜合報導〕電信詐騙推陳出新，新一波的詐騙簡訊App要求使用者「下載」程式才能查看照相或罰單紀錄；也有歹徒冒名警察局發簡訊詐騙，有人點擊連結沒有反應，連點了10次，收到帳單才發現被騙了1萬元。



誤點詐騙簡訊，被害人收到萬元帳單。（記者何宗翰翻攝）

刑事局指出，近期出現以手機簡訊、LINE及WeChat（微信）發送「您的汽機車有交通罰單未繳，查一查自己有無莫名被照相或罰款的紀錄」，有民眾一時好奇，依指示下載App，等隔月收到帳單無故多了「小額付款交易」，才知是詐騙伎倆。

新竹市警局中華派出所本月接獲10起網路詐騙案，全都是以「新北市警察局」名義，發簡訊詐騙，有人還因點擊10次，被騙1萬元。

刑事局呼籲，不管這些惡意程式包著什麼糖衣，不要點選任何連結，才是自保的不二法

運動 娛樂 生活

篇

享 讚 2

法，這次鎖定有車一族。新
詢問是否有罰單逾期未繳的
收到查詢罰款紀錄的簡訊，

未繳納，查一查自己有無莫
載http://g--.gl/VamU-

額增加，因此特別提醒車
要竊取民眾的個資。

對被舉發事實有疑義時，可
出等相關資料，完成申訴程

立74歲郭姓老婦人，接獲電
言保管，以利案件偵辦，甚

新聞事件

宅急便病毒化身35種簡訊　一人中鏢好友恐全難逃

NOWnews – 2014年6月24日 上午11:13

記者李鴻典／台北報導

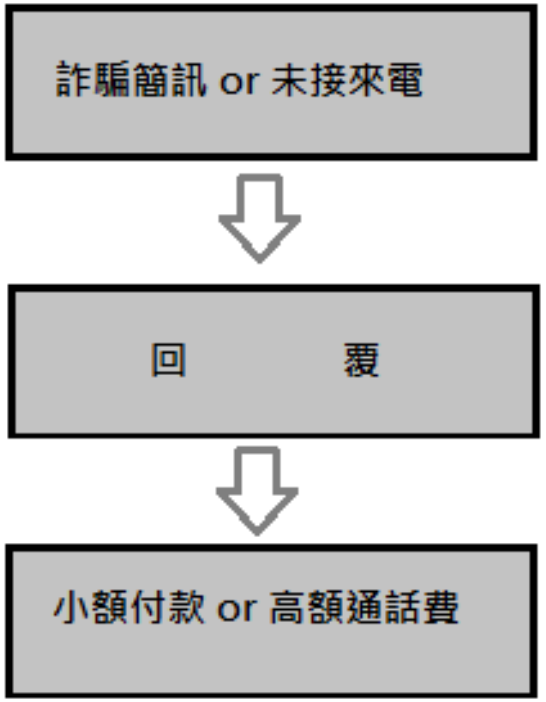
日前曾肆虐一時的宅急便病毒，近期出現了各式各樣、多達35款的新型變種簡訊！主要是透過各種引人注目的文字內容，例如「來下載上次聚會的照片」、冒充「新北市政府警察局」的案件處理結果通知單、「張惠妹新歌試聽」等等，在簡訊中放入含有病毒的網址連結，誘使民眾點擊。

近來，各地警察局紛紛接獲報案，已有不少民眾受害，損失金額甚至達萬元。若民眾不小心受簡訊內容引誘，點進該病毒連結，就會被誘導下載「小額支付大盜App」，直接導致金錢損失。

行動應用程式開發商獵豹移動（Cheetah Mobile）指出，上個月宅急便病毒正流行的時期，在台灣一天約偵測到4000位使用者收到此類簡訊，但近期由於變種病毒以各種形式大流行，每天會收到病毒簡訊的民眾已經暴增五倍。獵豹移動在Android平台的免費手機防毒軟體CM Security，就偵測到一天最多有2萬人受害。

為了保障使用者的手機安全，CM Security特別針對此詐騙形式，推出掃描簡訊連結、攔截

簡訊詐騙流程 (傳統)



Edwin 說:
- 阿~你現在可以收簡訊嗎？

小捲芋泥 (oo)ﾉ 說:
- 可以啊 怎麼了

Edwin 說:
- ~那個簡訊不是我傳給你拉

我手機摔壞了＝＝
我現在想申請奇摩Y拍的帳號
需要手機驗證碼 你幫我收一下?

小捲芋泥 (oo)ﾉ 說:
- 怎驗證阿

資訊服務經營者節目費上限

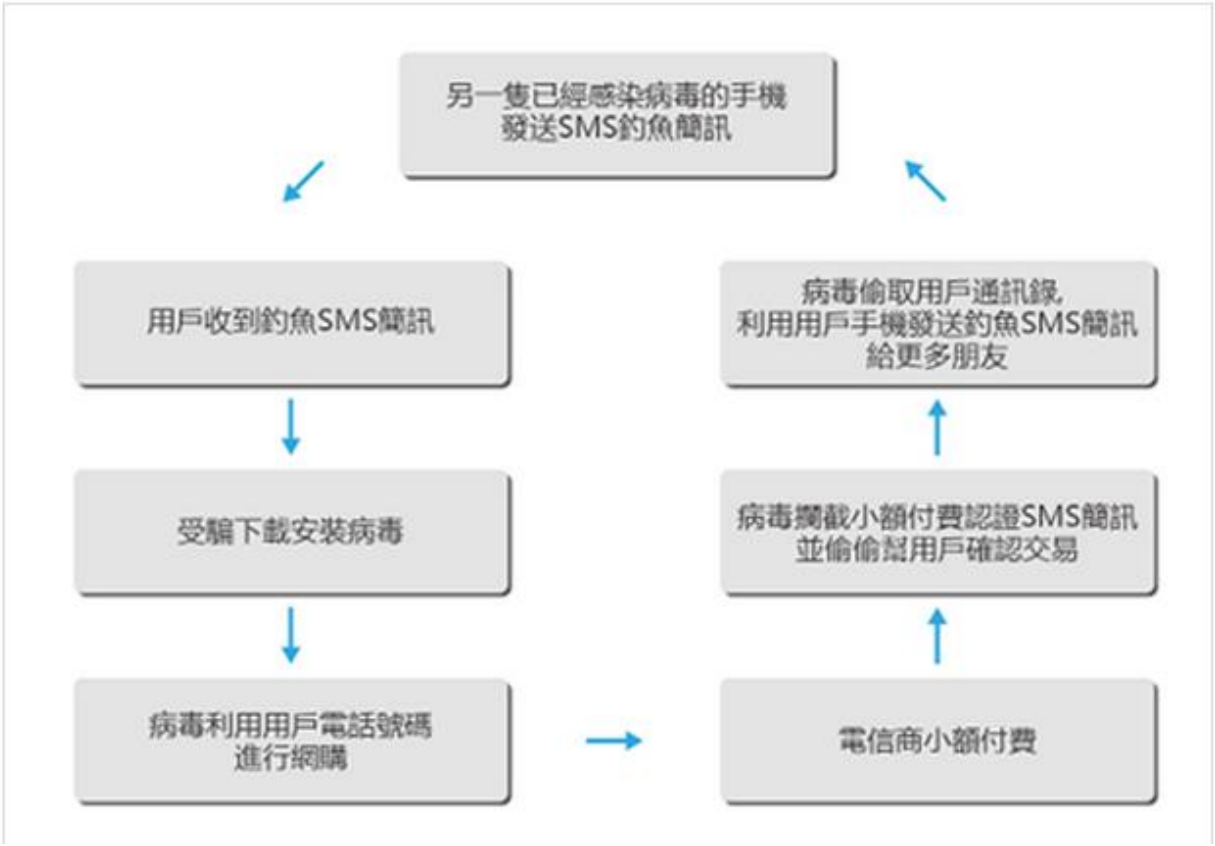
一、 兒童節目：每分鐘十元，每
二、 會議專線：每分鐘二十元，
三、 專業諮詢：
專人諮詢：每分鐘一百元，
專業資訊：每分鐘三十元，
四、 仲介節目：每分鐘五十元，
五、 募款節目：每次一百元。
六、 娛樂節目：每分鐘二十元。
七、 電話投票：每次十元。
八、 語音播放節目：每分鐘十元

中華電信	每25秒1元	060、070、094200-98、0950、0957、0959
	每25秒2元	094299
大眾電信	每30秒2元	09481-3、09485-6、09488-9
聯華電信	每10秒1元	09450-1
	每25秒1元	09463
	每30秒2元	09430-3、09435-9、09455-9、09461、09465-8、09455-9、09461、09465-8
中華國際	每分1.5元	095104
	每分2元	095129
	每30秒2元	094100-9、094110-9、094130-2、095106-8
	每分4元	094120-1、094123-9、094150-2、094190-9、095100-3、095105、095130-4
	每分6元	094122、094133-9、094140-9、094153-9、094160-9、094170-9、094180-9、095109、095110-9、095120-8、095135-6、095138-9
	每分8元	095137

申請取消小額付費服務


台灣大哥大
行動用戶 | 家庭用戶 | 企業用戶 | 關於我們 | 基金會 | 品牌故事 | myfone購物
ENGLISH
行動版
搜尋
網路門市
資費&手機
用戶服務
享優惠
APP&加值
出國去
查維修
4G LTE
我的帳單/繳費 | 我的資費/變更 | 我的合約/續約 | 國際漫遊/申請 | 我的服務/優惠 | 預付卡餘額/儲值 | 手機專區&消費者課程 | 連絡我們 | 掛失
首頁 » 用戶服務 » 我的帳單/繳費 » 小額付款服務 » 可用額度查詢
用戶服務
我的帳單/繳費
總覽頁
查詢
帳單金額
近六期帳單
線上繳費
線上繳費紀錄
繳費(入帳)紀錄查詢
查詢未出帳/傳輸量
通話&上網明細
網路ATM轉帳繳款
轉帳/匯款繳費帳號
電信帳單代收
小額付款服務&消費紀錄
預付卡餘額/儲值
小額付款服務
交易記錄查詢
發票查詢
可用額度查詢
發票索取設定
統一發票處理說明
台灣大哥大/泛亞電信/東信電訊 小額付費可用額度查詢
歡迎光臨
您本月的可用額度為： 1000元
您目前的可用額度為： 1000元
額度說明：
1.每位客戶額度計算週期為每月1日~月底
2.當月可用額度可於CATCH網站/我的CATCH查詢(www.catch.net.tw/wap.catch.net.tw)
3.額度上限由本公司依據客戶消費狀況核定,本公司保留隨時異動的權利
備註:部份合作廠商可能另有額度限制,可用額度將因此減少.

簡訊詐騙流程(新型態)


另一隻已經感染病毒的手機
發送SMS釣魚簡訊
用戶收到釣魚SMS簡訊
受騙下載安裝病毒
病毒利用用戶電話號碼
進行網購
電信商小額付費
病毒擷截小額付費認證SMS簡訊
並偷偷幫用戶確認交易
病毒偷取用戶通訊錄,
利用用戶手機發送釣魚SMS簡訊
給更多朋友


+8869
2014/03/10 週一
您的快遞簽收通知單,收件電子憑證(http://goo.gl/1MN94O)
10:46
點我一下 ClickMe.net


2013/11/05 TUE
朋友家貓貓參加人氣比拼 幫忙贊一下
感恩
http://kin050s4.h-s15-host.eoisl.com/Info/View_Asp?id=718
PM 7:07
Ok
PM 7:07

最難纏「隱形且防刪除」Android木馬,取得系統最高權限恣意竊取手機資訊、訂購高付費服務，操控手機下載更多惡意程式

發表於 2013 年 06 月 19 日 由 Trend Labs 趨勢科技全球技術支援與研發中心

趨勢科技提供免費工具解除權限 搭配資安軟體即可阻止木馬屠城

【2013年06月19日 台北訊】最新會隱形Android木馬**ANDROIDOS_OBAD**現蹤，目前已知**ANDROIDOS_OBAD**透過論壇、WiFi，以及藍芽等方式傳遞，會攻擊Android系統漏洞，一旦安裝成功將會擁有設備管理員的權限，駭客將可完全掌控感染手機，恣意竊取手機資訊、訂購高付費服務，並可能操控手機下載更多惡意程式。趨勢科技(TSE:4704)提供免費工具「**Hidden Device Admin Detector app**.」協助解除該木馬所取得的最高權限，讓使用者可進一步以資安軟體清除該木馬程式。

五大手機病毒延燒　單月2萬台Android手機遭駭

NOWnews – 2014年6月5日 下午1:10

字 +字

記者李鴻典／台北報導

手機病毒持續蔓延！CM (Clean Master) Security安全實驗室今(5)日在臺發佈《全球五月份安全月報》，資料顯示，五月份是宅急便病毒、Google服務病毒、手機遊戲病毒肆虐的高峰，過去一個月內，全台遭受病毒感染的Android手機已經高達2萬台。

CM Security實驗室鄭重呼籲，宅急便病毒已經變種偽裝成Google應用服務，病毒散播甚至已蔓延至Facebook，用戶應避免點選來路不明的連結，或在GooglePlay以外的平臺下載軟體，以免手機被植入病毒而不自知。

亞洲地區對於手機應用軟體的管制門檻較低，成為全球手機病毒的重要發源地。根據CM Security實驗室發佈的《全球五月

“48小時內支付贖金，否則你手機上的所有資料將永久被破壞！”又一手機勒索軟體現身

發表於 2014 年 06 月 25 日 由 Trend Labs 趨勢科技全球技術支

Tweet 0 | +1 0 | 分享 2 | 讚

讚 2 | +1 0 | 推文 0

Android勒索軟體利用Tor隱藏C&C通訊

不久前我們介紹過不給錢就讓手機變磚塊!勒索
最近出現在行動威脅環境的勒索軟體現在有了
名服務來隱藏C&C通訊。

За скачивание и установку нелицензионнного ПО ваш телефон был ЗАБЛОКИРОВАН в соответствии со статьей 1252 ГК РФ Защита исключительных прав. Для разблокировки вашего телефона оплатите 1000 руб. У вас есть 48 часов на оплату, в противном случае все данные с вашего телефона будут безвозвратно уничтожены!

1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79660624806 и нажмите далее
4. Появится окно коментарий - тут введите ВАШ номер телефона без 7ки
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 24 Часов после поступления платежа ваш телефон будет разблокирован.
7. Так же вы можете оплатить через салоны связи Связной и Евросеть

ВНИМАНИЕ: Попытки разблокировать телефон самостоятельно приведут к полной полной блокировке вашего телефона, и потери всей информации без дальнейшей возможности разблокирования.

詐騙簡訊類型

- 需要即時確認

「○○○女士您有交通罰單逾期未繳...」
「○○○先生,你的露天商品已經送達門市...」
「您的快遞簽收通知單，收件電子憑證」

- 「好奇想要確認」

「看看那些年我們合拍的照片是多麼年輕」
「○○○這是上次聚會的照片，你好好笑」
「○○○看著這些照片，好懷念以前的日子！」
「○○○我們中秋烤肉的照片,好多人喔」

詐騙簡訊類型

- 「嚇唬你讓你想確認」

【新北市政府警察局通知單】您涉嫌的案件處理結果通知單。
「尊敬的客戶您好，您的手機正在申請6800元的網絡支付，如非本人操作請加載電子憑證確認取消...」
。
你的民事賠償訴訟通知單【台北地院】。

- 「免費貼圖、人氣投票或按讚」

“fb 免費送貼圖,把此消息轉發十五個 LINE 好友,可以免費領取價值一百的貼圖表情,加油吧,領取地址...”
「○○○朋友家狗狗參加人氣比拼，幫忙讚一下」
「學運受傷學生急需醫藥費！」
「我的手機送修，麻煩替我收個簡訊好嗎？」
「拜託收幾封購物簡訊，我有急用！」

Line免費貼圖詐騙


FB免費送貼圖 把此消息轉發15個Line好友
可以免費領取 價值一百的貼圖表情 加油吧
waroo
Smile Brush 2
facebook
電子郵件或電話
密碼

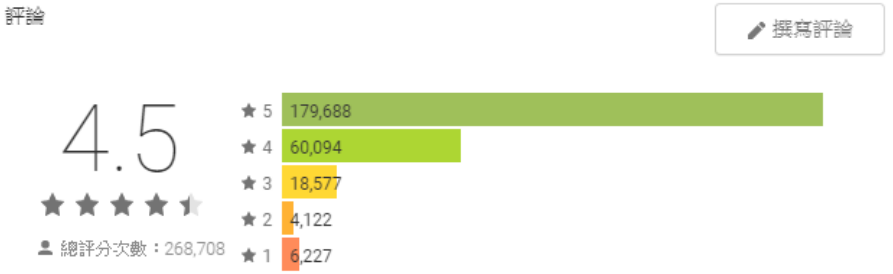
惡意QR Code

- 絕大多數的QR碼都是正常的，是企業用來和大眾互動的有趣模式。但還是有惡意QR碼的存在，而且如果它們跟我們之前見過的其他類型垃圾郵件(SPAM)一樣的話，那可以預期的是它們只會越變越多。

如何下載安全的軟體

僅供參考，並非絕對

- 僅從google play下載
- 評價



- 有無公司或提供者資訊是否有其他APP上架
- 安裝次數
- 知名廠商
- 問同事、朋友

安裝行動裝置防毒


16:51
安全達人
檢查中
91%
正在掃瞄：
LINE
已掃瞄檔案數目： 8
發現的威脅數目： 0
找到私密資料威脅： 3
取消
授權合約
拒絕
登入

極 機 密
Restricted & Confidential

FAR EASTONE
遠傳

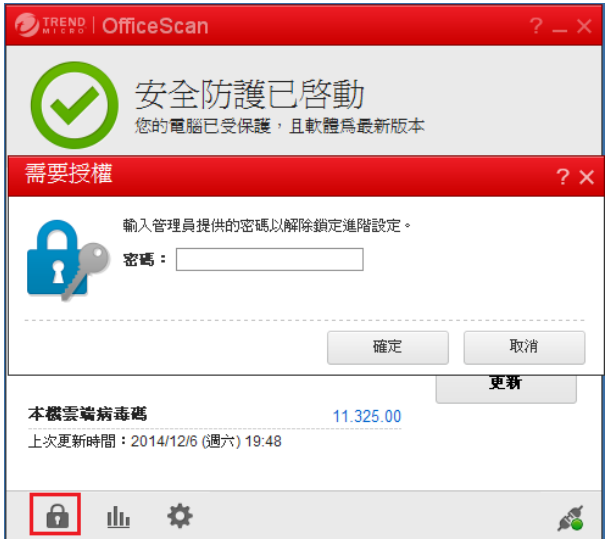
Mobile · Broadband · Media · International Service

OSCE 11用戶端畫面

OSCE11新用戶端介面

新用戶端介面

- [解除鎖定]用於啟動可能由管理員限制的所有功能。



❑ Q & A

補充資料

- 網頁:
  - 官方網頁http://www.trendmicro.tw/
  - 下載專區 http://downloadcenter.trendmicro.com/index.php?regs=TW
  - 教學影音http://esupport.trendmicro.com/zh-tw/business/topic_knowledgedownload.aspx
  - 技術支援資料庫http://esupport.trendmicro.com/zh-tw/business/topic_techsupport.aspx
  - **＊技術支援**http://esupport.trendmicro.com/zh-tw/srf/twbizmain.aspx

- 電話:
  - ＊技術支援:02-2377-2323#1

Thank You!