安全的使用個人電腦

個人電腦防護與網路安全

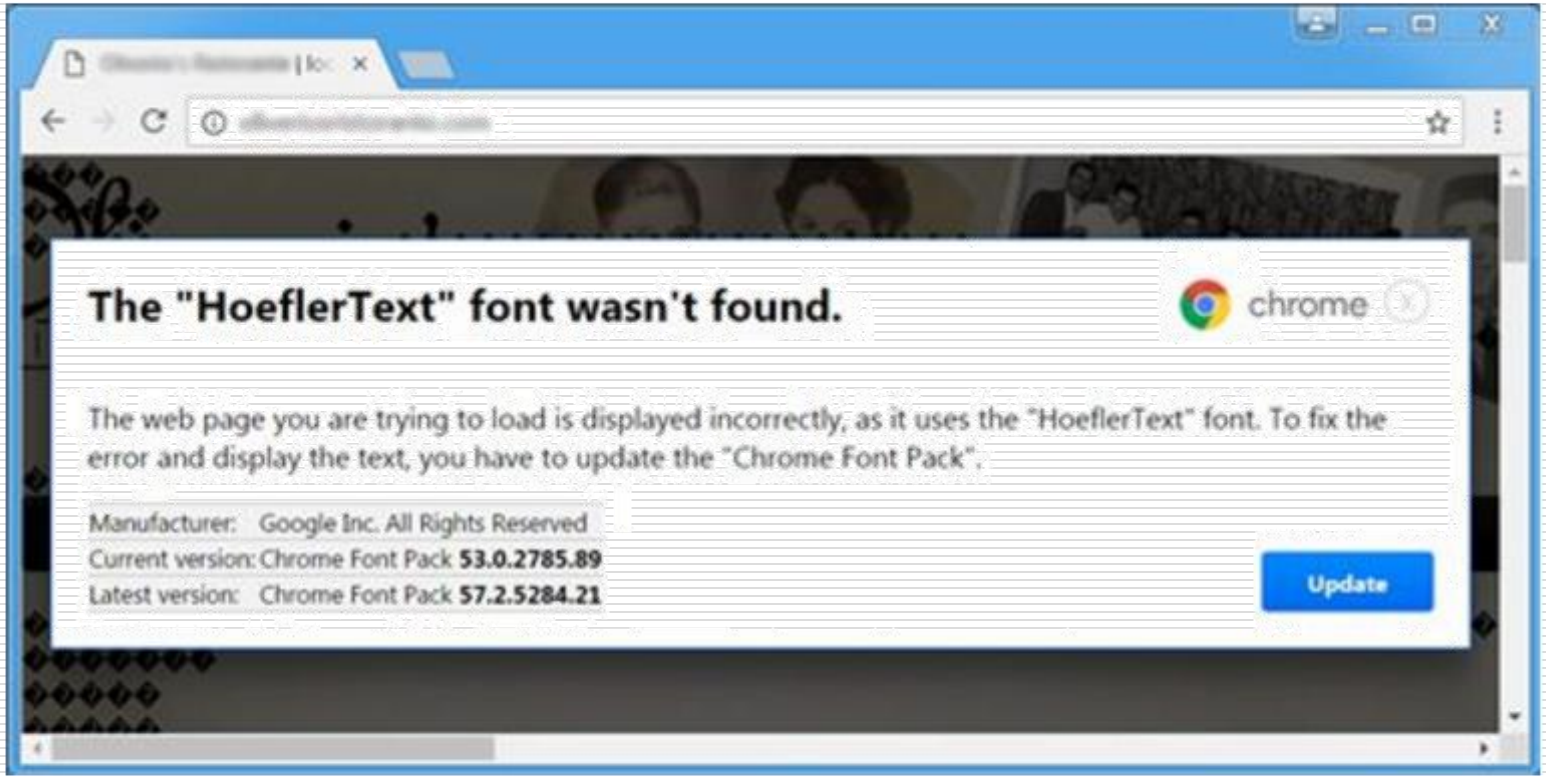
資訊處　網路管理組　張維廷

2017.4.20

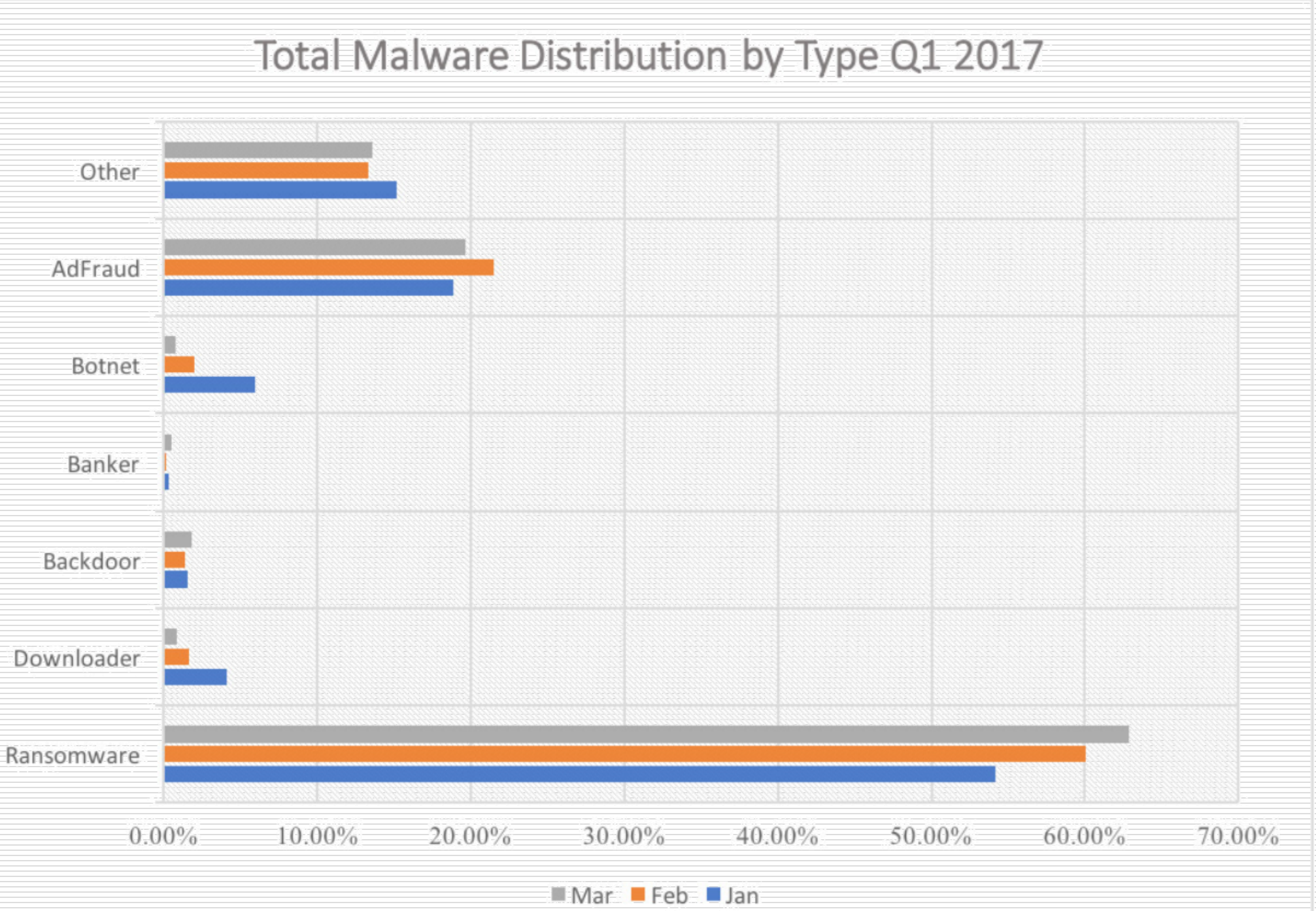
Chrome要你更新字型別亂按　恐掉入勒索病毒陷阱

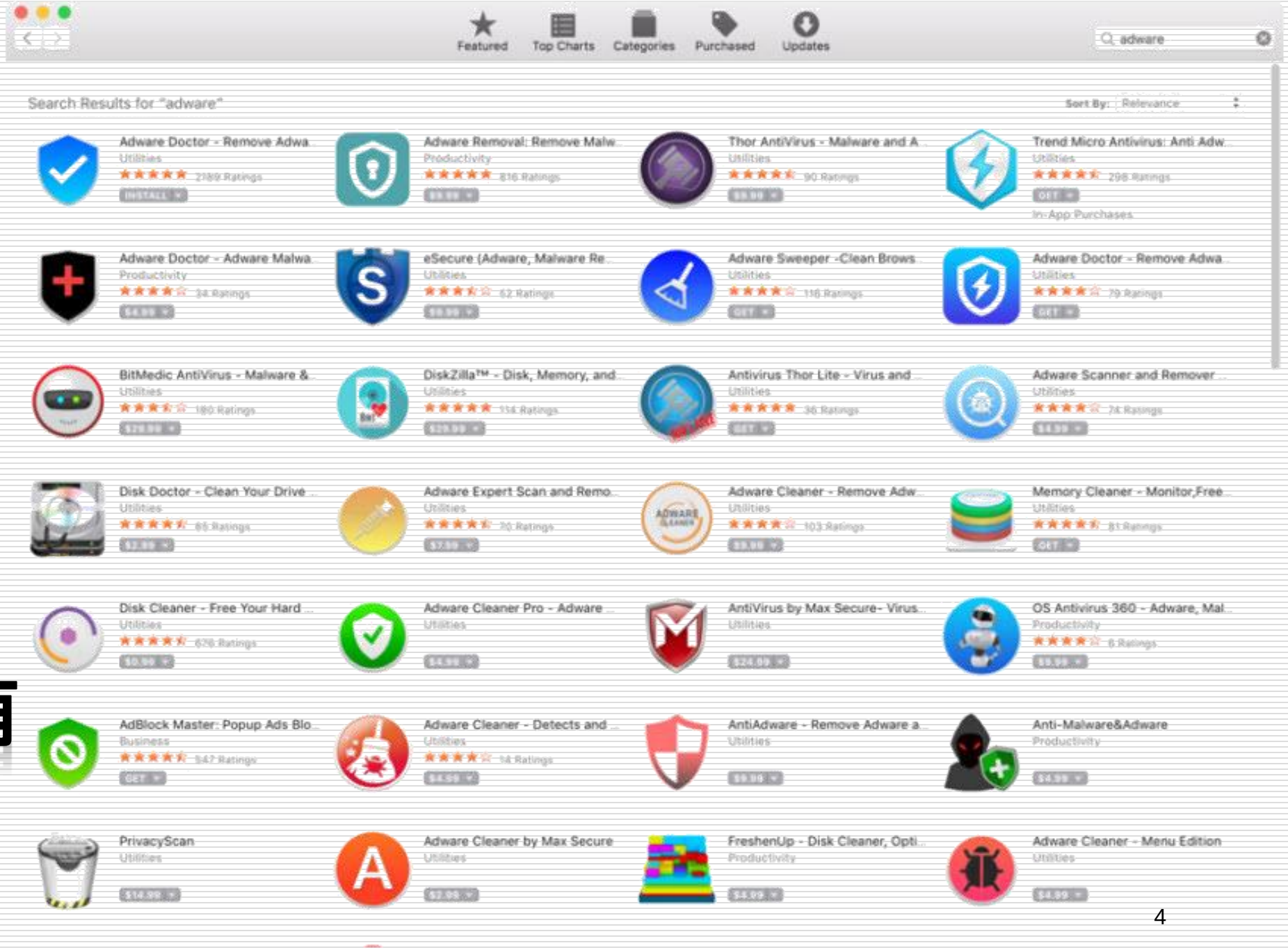
中央社　2017/04/15 09:17:00　友善列印　加入好友　讚 4,636　G+1 5　A- A A+

網路資安廠商趨勢科技提醒消費者，使用Google Chrome瀏覽器如果彈出「找不到字型」視窗，別急著按更新，小心可能是勒索病毒假冒的。



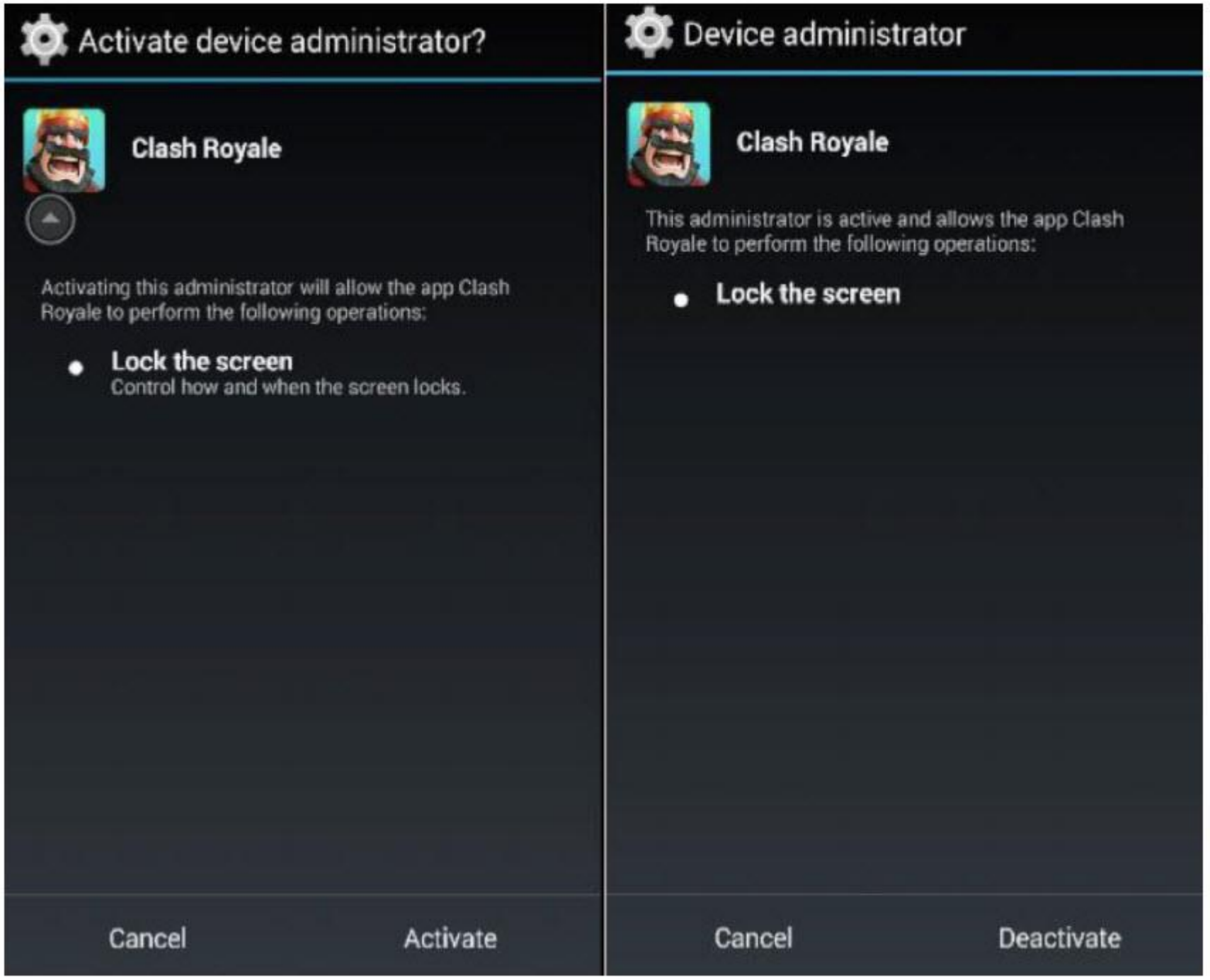
▲圖 / 中央社


Total Malware Distribution by Type Q1 2017
Other
AdFraud
Botnet
Banker
Backdoor
Downloader
Ransomware
0.00%
10.00%
20.00%
30.00%
40.00%
50.00%
60.00%
70.00%
Mar
Feb
Jan



不要以為只有WINDOWS會中毒

ANDROID也很危險



你被勒索了嗎?

CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

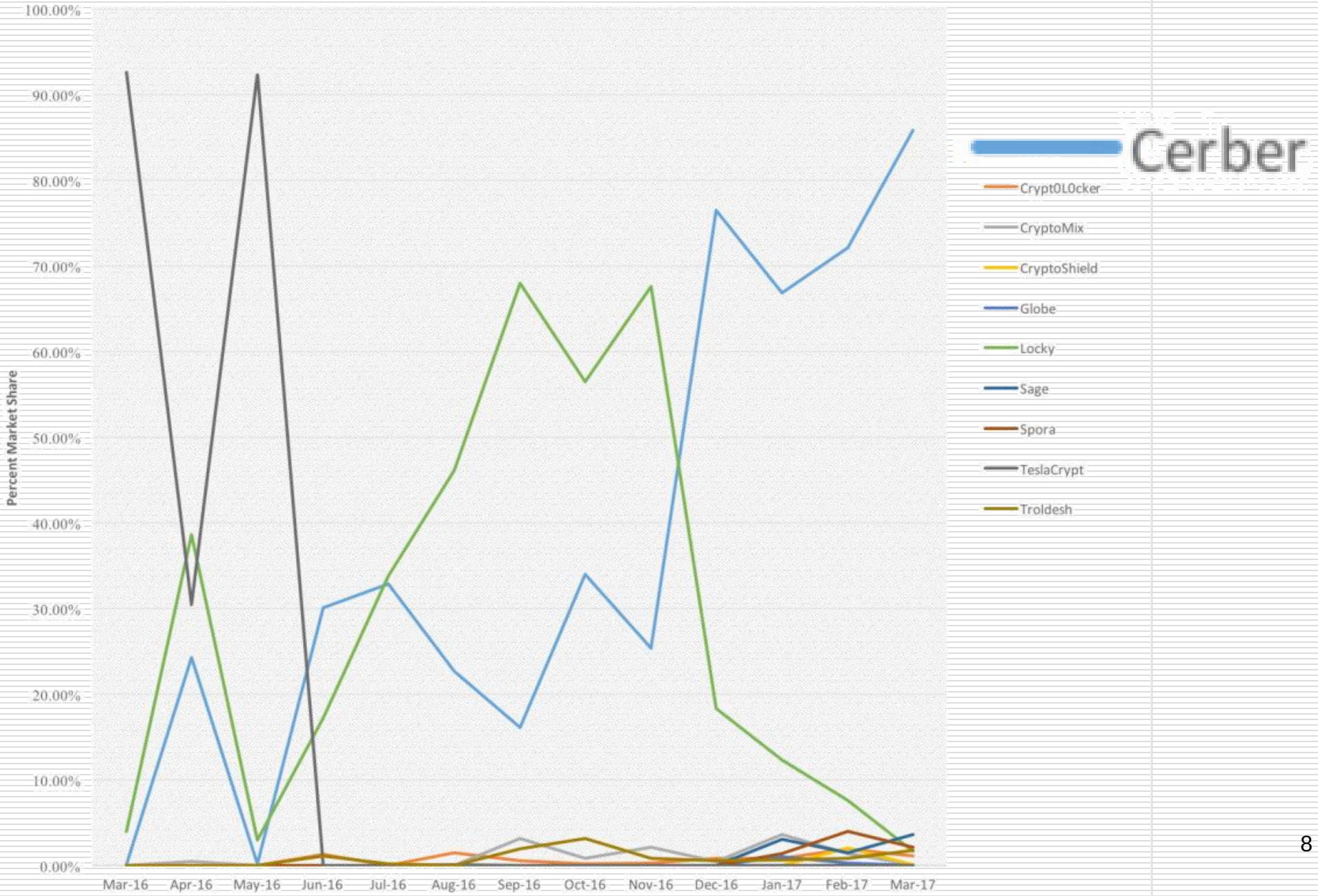
To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*_READ_THIS_FILE_*)
with complete instructions how to decrypt your files.

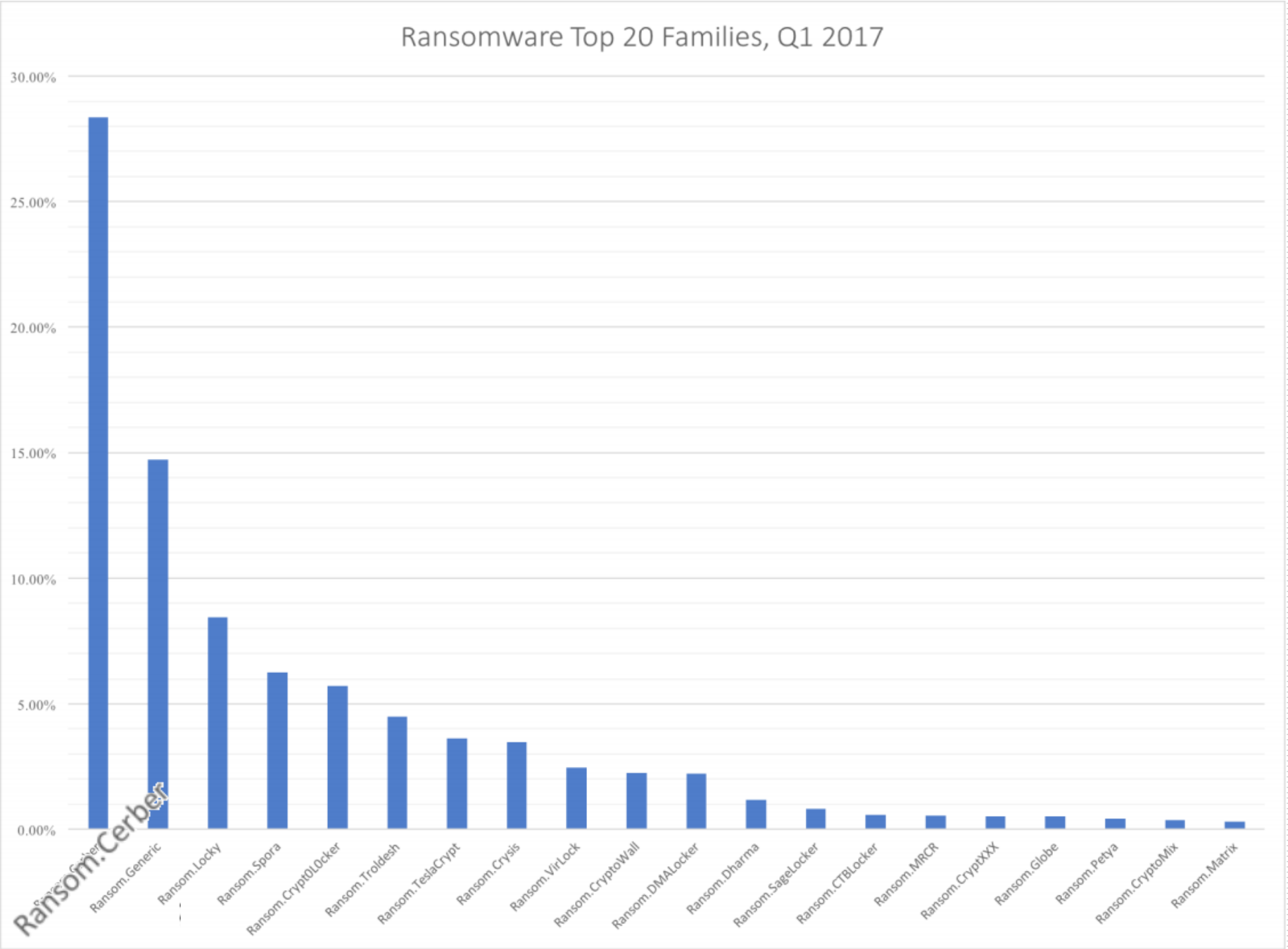
If you cannot find any (*_READ_THIS_FILE_*) file at your PC,
follow the instructions below:

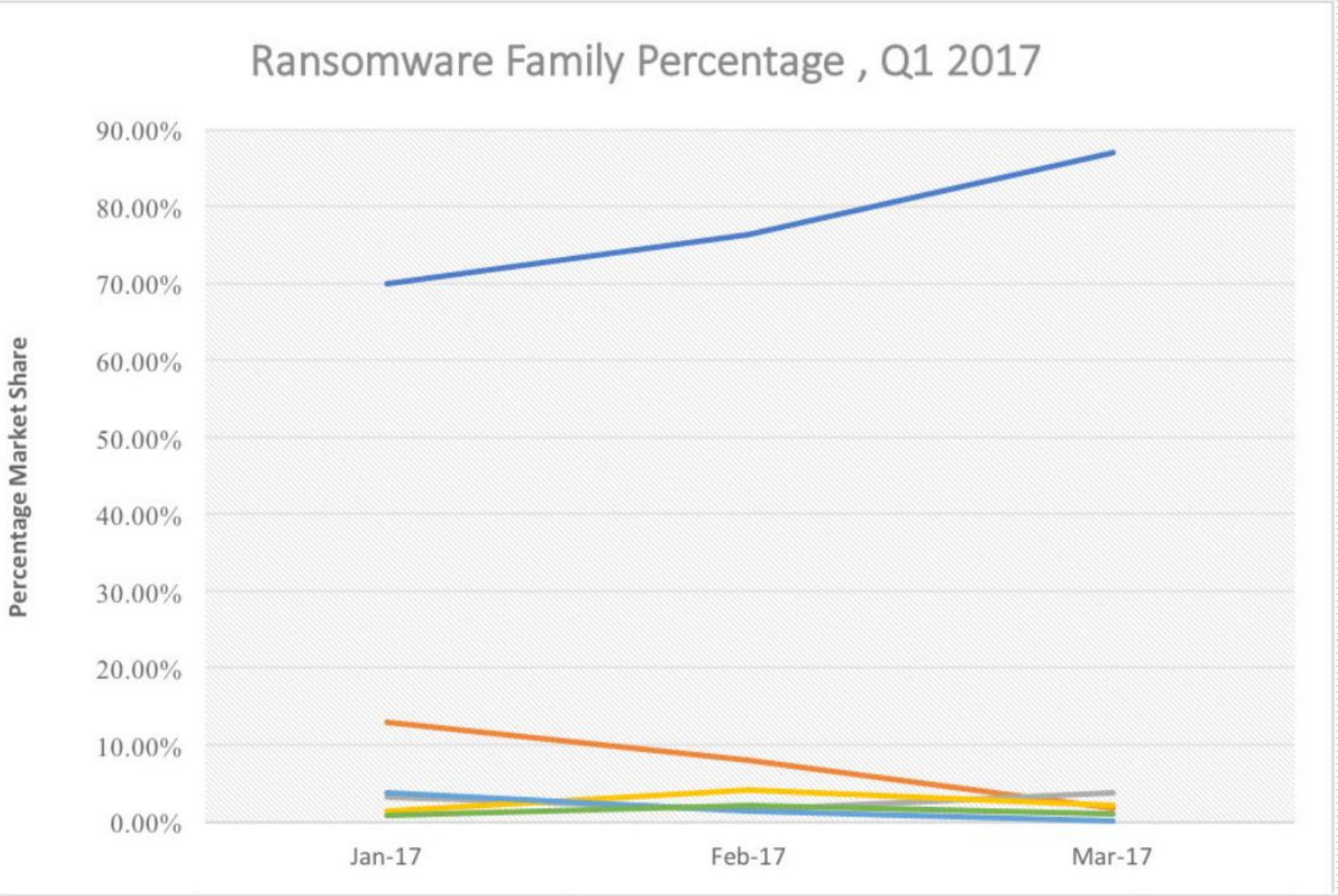
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

[redacted]

Note! This page is available via "Tor Browser" only.


12 Month Ransmoware Family Trends 2016/2017
Percent Market Share
100.00%
90.00%
80.00%
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
Mar-16
Apr-16
May-16
Jun-16
Jul-16
Aug-16
Sep-16
Oct-16
Nov-16
Dec-16
Jan-17
Feb-17
Mar-17
Cerber
Crypt0L0cker
CryptoMix
CryptoShield
Globe
Locky
Sage
Spora
TeslaCrypt
Troldesh


Ransomware Top 20 Families, Q1 2017
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
Ransom.Cerber
Ransom.Generic
Ransom.Locky
Ransom.Spora
Ransom.Crypt0L0cker
Ransom.Troldesh
Ransom.TeslaCrypt
Ransom.Crysis
Ransom.VirLock
Ransom.CryptoWall
Ransom.DMALocker
Ransom.Dharma
Ransom.SageLocker
Ransom.CTBLocker
Ransom.MRCR
Ransom.CryptXXX
Ransom.Globe
Ransom.Petya
Ransom.CryptoMix
Ransom.Matrix



	Jan-17	Feb-17	Mar-17
Cerber	70.05%	76.29%	86.98%
Sage	3.17%	1.57%	3.69%
Spora	1.47%	4.15%	2.14%
CryptoMix	3.79%	1.43%	0.07%
CryptOL0cker	0.85%	2.06%	1.11%

RANSOMWARE 勒索軟體

- 近來最猖獗，不容忽視的安全議題
- 高達 95%以上的企業，其使用者都曾經遇到這樣的問題
- 導致資料與財務的損失，造成非常嚴重的困擾。

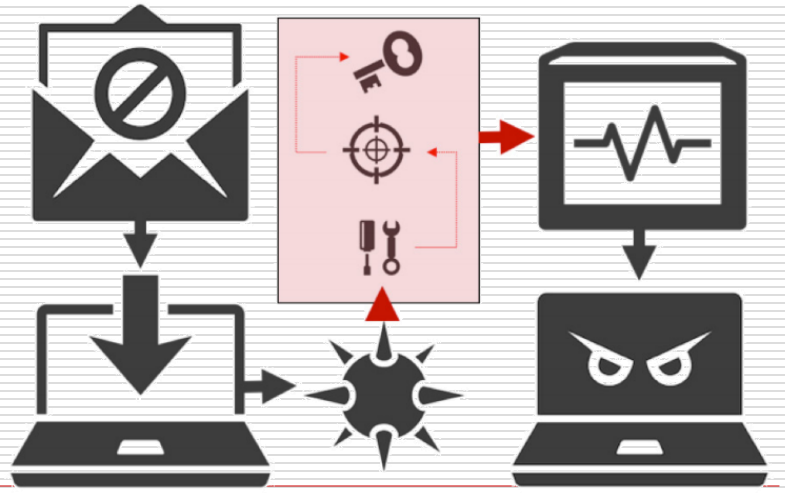
為何勒索軟體如此猖獗？

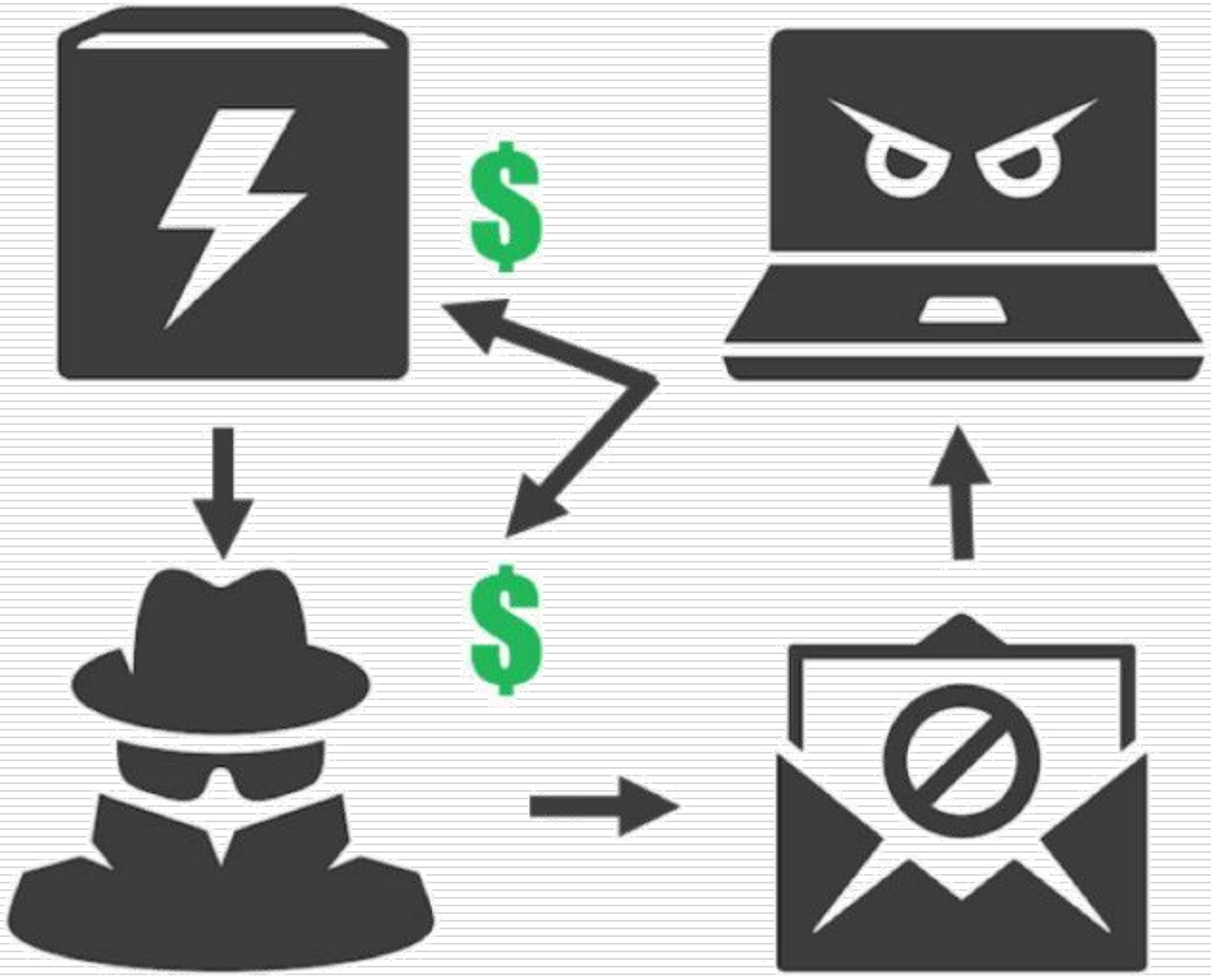
- 四通八達的網路環境是一大助力。
- 跳脫傳統框架且兼具便利與安全的跨國金融流通管道。
- 即時、方便好用的付款方式正好讓犯罪者們可以輕鬆收取贖金，加上有些金融移轉系統具有匿名性，有助於駭客將自己充分隱匿起來。

勒索軟體如何散佈？

- 大量利用電子郵件、網頁與應用程式下載來進行散佈。

- 在未受到妥善安全防護的網站，利用弱點植入感染程序，讓使用者在上網完全沒有察覺的情況下，遭受感染植入，並間接透過社交行為擴散給其他機器 。





Ransomware as a Service

真的不幸中獎了怎麼辦?

面對日益嚴重的資安威脅，

您準備好了嗎?

個人電腦防護

先來談談密碼吧!

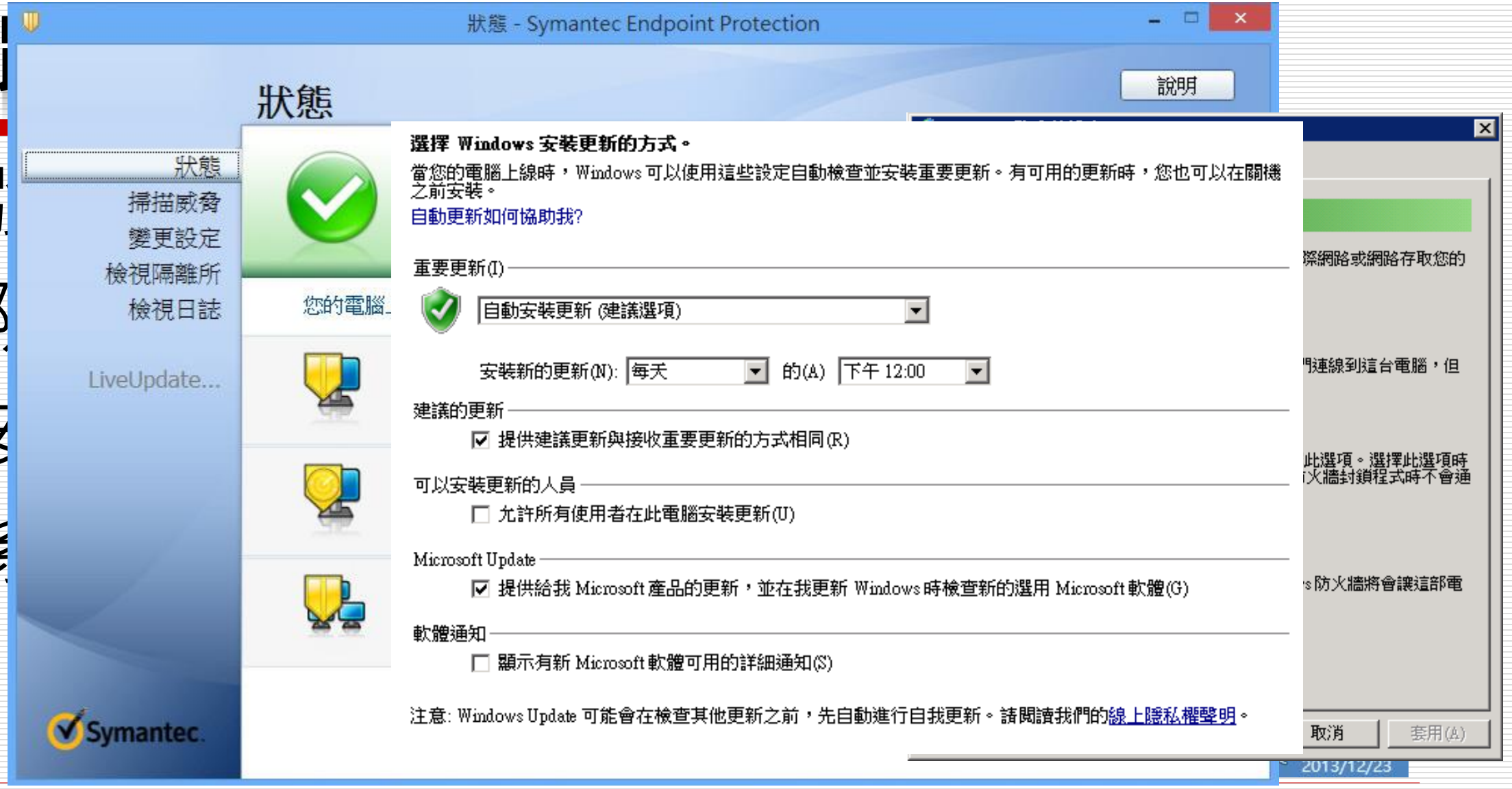
- 密碼是抵禦攻擊的第一道防線。
- 對每個重要帳號使用不同密碼
- 挑選安全強度高的密碼以及定期加以變更，是非常重要的事。
- 密碼原則
- 強度測試

個人電腦防護

- 個人電腦防護分為兩個層面：
  - 網路防護
  - 資料防護

網

- □弱
- □防
- □安
- □系


狀態 - Symantec Endpoint Protection
說明
狀態
狀態
掃描威脅
變更設定
檢視隔離所
檢視日誌
LiveUpdate...
您的電腦
Symantec.
選擇 Windows 安裝更新的方式。
當您的電腦上線時，Windows 可以使用這些設定自動檢查並安裝重要更新。有可用的更新時，您也可以在關機之前安裝。
自動更新如何協助我?
重要更新(I)
自動安裝更新 (建議選項)
安裝新的更新(N): 每天 的(A) 下午 12:00
建議的更新
提供建議更新與接收重要更新的方式相同(R)
可以安裝更新的人員
允許所有使用者在此電腦安裝更新(U)
Microsoft Update
提供給我 Microsoft 產品的更新，並在我更新 Windows 時檢查新的選用 Microsoft 軟體(G)
軟體通知
顯示有新 Microsoft 軟體可用的詳細通知(S)
注意: Windows Update 可能會在檢查其他更新之前，先自動進行自我更新。請閱讀我們的線上隱私權聲明。
取消
套用(A)
2013/12/23

資料防護

- 設定開機密碼
- 設定螢幕保護密碼
- 除了惡意入侵，導致資料外流或遭破壞，是否還有其他可能?

養成檔案備份的好習慣

檔案備份

- 應定期備份個人電腦設備內重要文件及資訊。
- 可藉由
  - 不同的儲存媒體
  - 各式各樣的工具軟體
  - Windows本身所提供的程式

  達到備份的目的

製作備份

- 排程備份工作
- 建立系統映像檔案
- 建立系統修復光碟
- 雲端備份

檔案的隱私

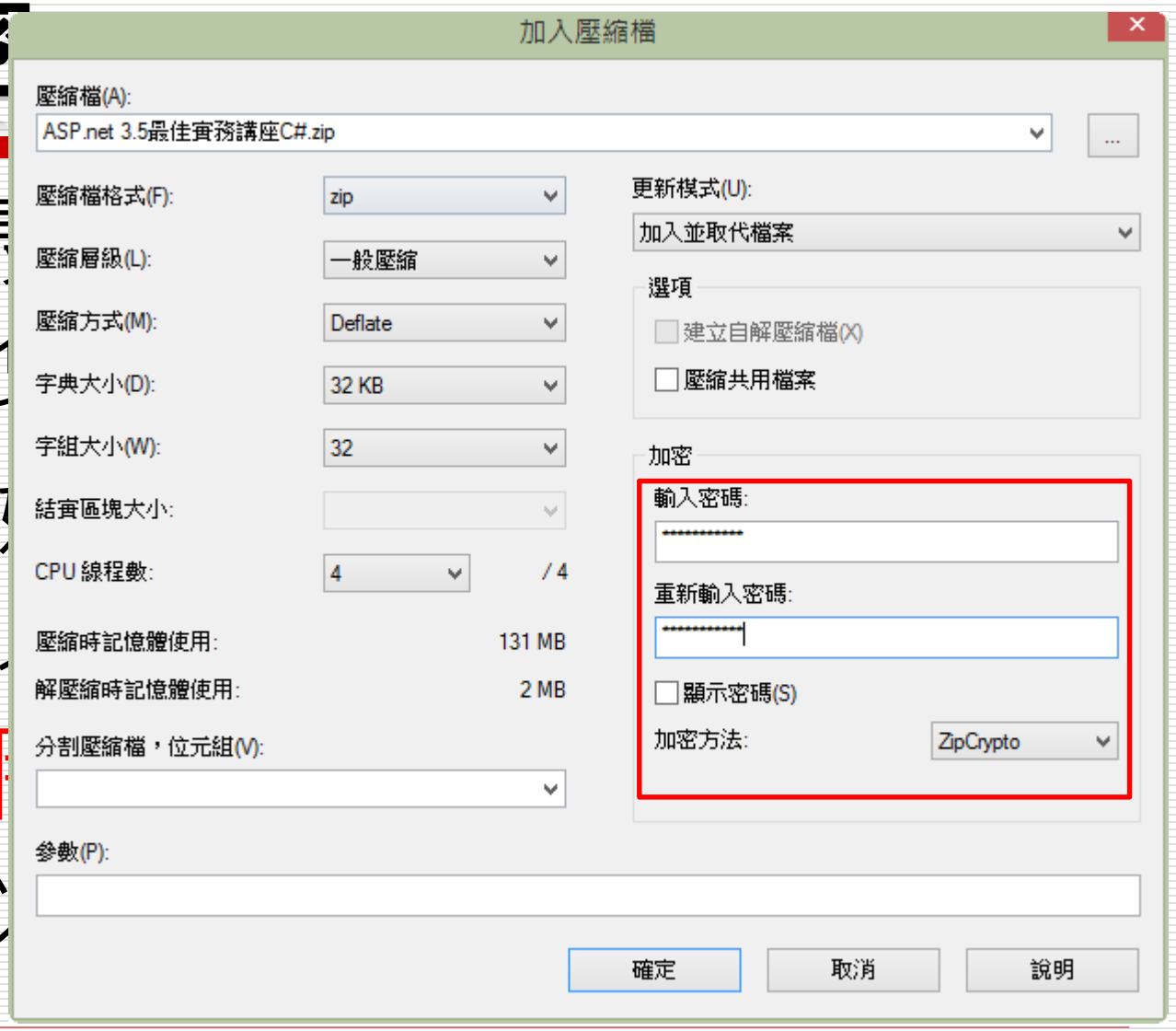
- 管理檔案的安全性原則
- 檔案與資料夾加密

管理檔案的安全性原則

- 進行下載、複製、使用不明來源檔案請集中單一資料夾管理並先完成掃毒。

檔案與資料夾加密

- 加密是 Windows 最
  護資料的安全，並
- 儲存於可攜式儲存
  關電子檔案也應予
- 電子檔案如須於網
  必須加密處理，以



網路安全

家庭WI-FI未設密碼 遭歹徒借用盜刷

2013年12月5日

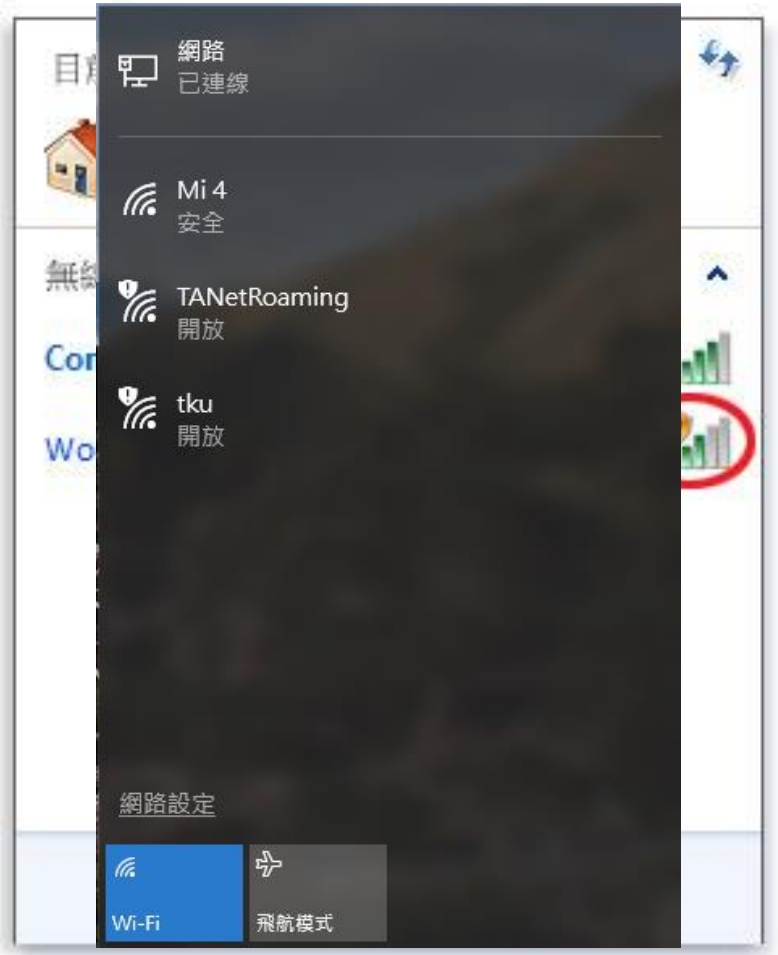
蘋果日報

你家的無線網路還沒設密碼嗎？

- 「反正我家電腦也沒什麼機密資料，應該沒有駭客會這麼湊巧住在我家隔壁，想來入侵我家的電腦吧？」
- 「每次朋友來要用Wi-Fi，都還要記密碼好麻煩，有人要用就大方分享給他們用吧！」
- 警方依照刷卡時的IP鎖定了六個嫌犯，但是卻發現這六名「嫌犯」都只是單純的上班族、家庭主婦，甚至對於網路也沒什麼概念，一點都不像高科技的駭客。最後警方才發現，這些人的共通點都是：家中的無線網路沒有設密碼。

如何知道無線網路的安全性？

- 儘可能只連線到需要連線密碼的網路
- 在不安全的網路上會顯示保護盾圖示
- 如果您連線到不安全的網路，
  可能您的所有動作已經被監看了，
  包括瀏覽的網站、
  使用中的文件以及
  您的使用者名稱與密碼。



看似亂碼，其實是...

- 27.50.22.62 - - [22/Dec/2013:08:30:04 +0800] "POST /cgi-bin/php.cgi?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
- URL解譯

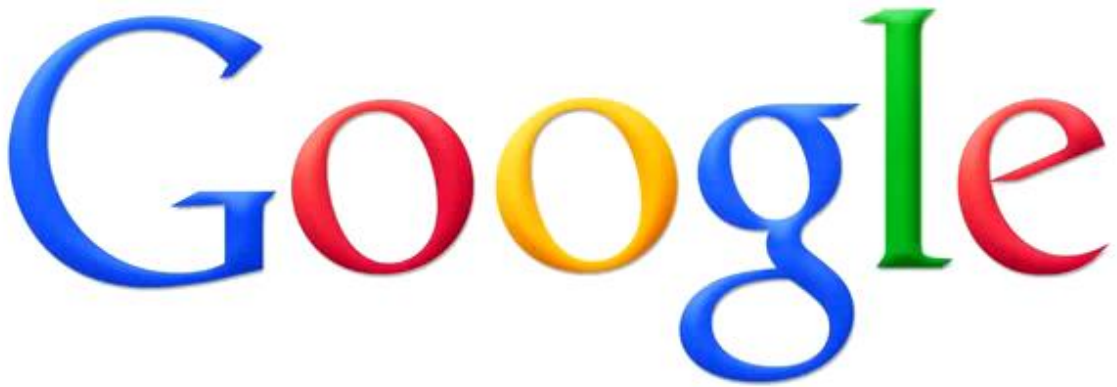
如何安心地上網

5 個確保網路安全的提示

- 使用強健的密碼
- 開啟兩階段驗證
- 立即安裝更新
- 可疑郵件要提高警覺
- 定期掃描

5 tips for staying safe on the web

1. Use strong passwords
2. Enable 2-step verification
3. Install updates right away
4. Be wary of suspicious emails and offers
5. Scan regularly for viruses


Google

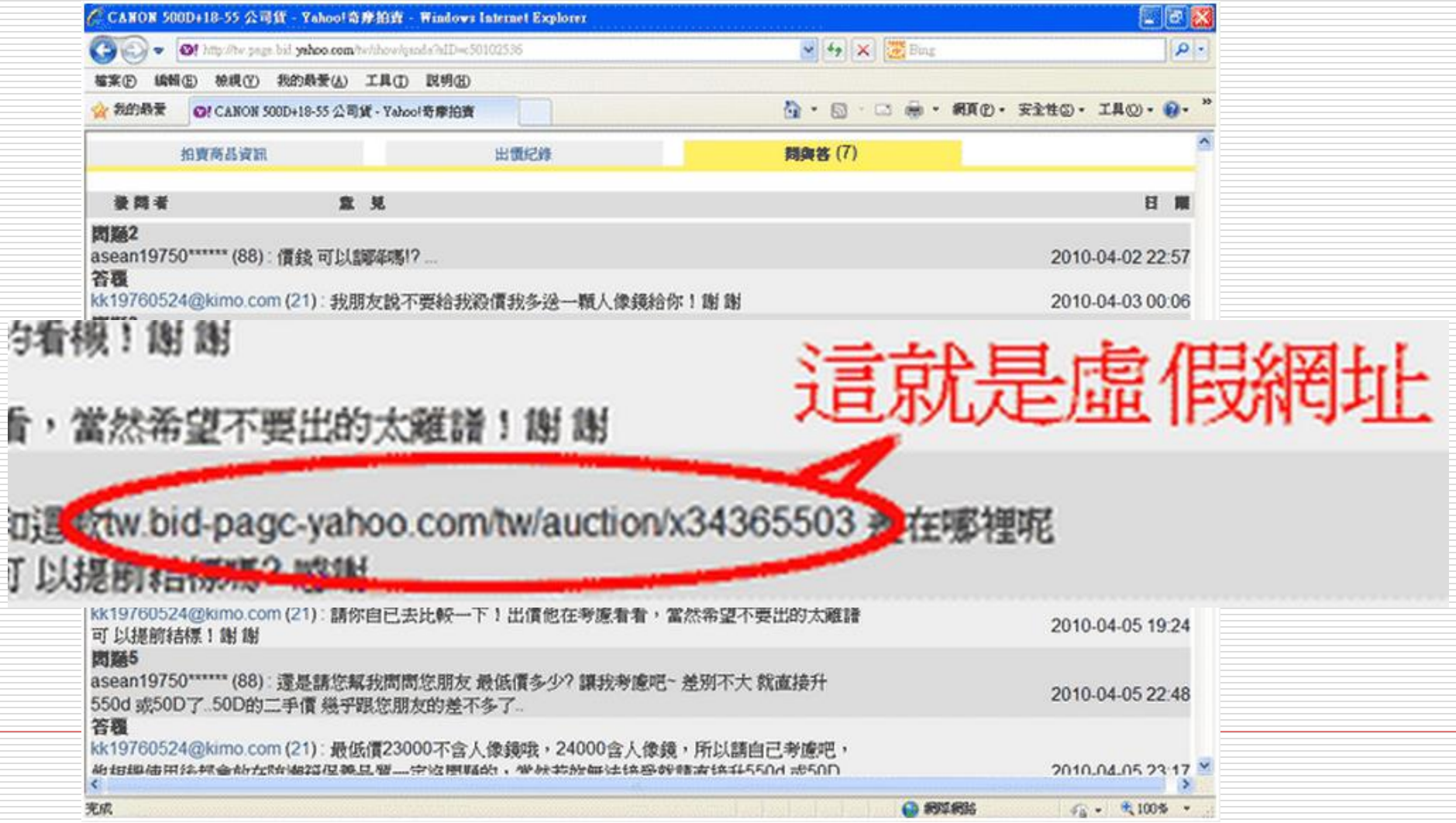
防止身分被盜用

- 如果看到可疑的郵件、即時訊息或網頁要求您提供個人資料，切勿回覆。
- 如果您是在郵件或即時通訊中點擊連結後前往某個網站，絕對不可輸入自己的密碼。
- 不要透過網路傳送您的密碼，也不要告知他人。
- 密切注意要求您登入的網站。

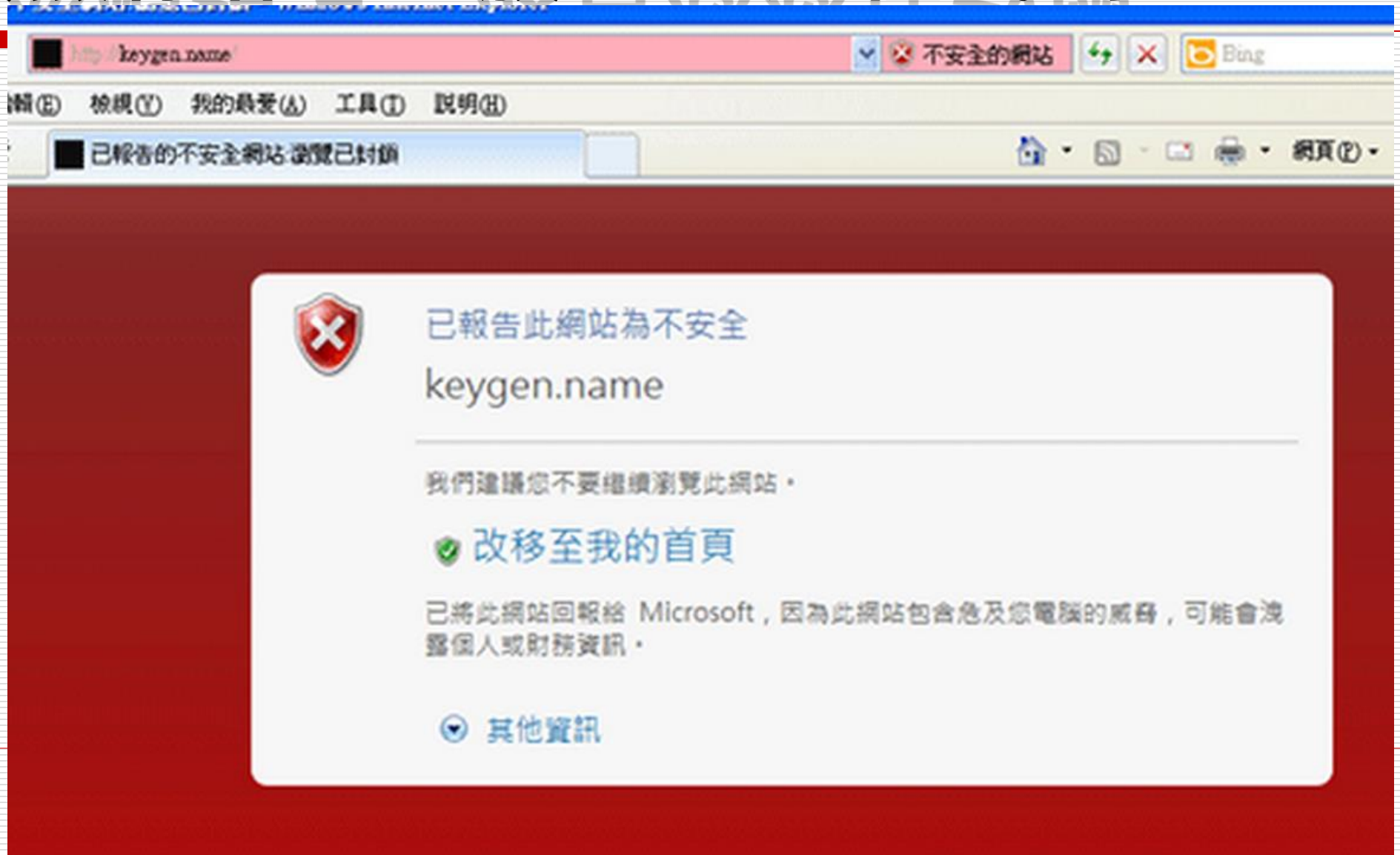
釣魚網站-1　虛構網站

- https://login.yahoo.com/config/mail?.intl=tw
- https://login-yahoo.com/config/mail?.intl=tw

釣魚網站-1　虛構網站


CANON 500D+18-55 公司貨 - Yahoo!奇摩拍賣 - Windows Internet Explorer
拍賣商品資訊
出價紀錄
問與答 (7)
發問者
意見
日期
問題2
asean19750****** (88) : 價錢 可以調降嗎!? ...
2010-04-02 22:57
答覆
kk19760524@kimo.com (21) : 我朋友說不要給我殺價我多送一顆人像鏡給你！謝 謝
2010-04-03 00:06
看機！謝 謝
，當然希望不要出的太離譜！謝 謝
這就是虛假網址
tw.bid-pagc-yahoo.com/tw/auction/x34365503
在哪裡呢
kk19760524@kimo.com (21) : 請你自己去比較一下！出價他在考慮看看，當然希望不要出的太離譜
可 以提前結標！謝 謝
2010-04-05 19:24
問題5
asean19750****** (88) : 還是請您幫我問問您朋友 最低價多少? 讓我考慮吧~ 差別不大 就直接升
550d 或50D了..50D的二手價 幾乎跟您朋友的差不多了..
2010-04-05 22:48
答覆
kk19760524@kimo.com (21) : 最低價23000不含人像鏡哦，24000含人像鏡，所以請自己考慮吧，
2010-04-05 23:17
完成

釣魚網站-2　放置惡意程式碼



釣魚網頁分辨測試


VeriSign
網釣
或 非網釣？
網釣網站看起來是什麼樣子？ 通常，就跟
真的網站沒什麼兩樣。 您是否能夠指出真實網站與
詐騙網站之間的差別？ 馬上透過這個簡短的測驗來測試您的能耐。

保護裝置免受入侵

- 隨時保持使用最新版本的瀏覽器和作業系統。
- 隨時注意您點擊或下載的內容，包括音樂、電影、檔案、瀏覽器外掛程式或附加功能。
- 請務必從可信任的來源取得要安裝的軟件。
- 如果電腦已感染到惡意軟件，請儘快移除。

瀏覽器與網路安全

- 紀錄(History)

帳號：

密碼：105167

登入

- 自動填充功能

您要 Internet Explorer 記住 tku.edu.tw 的密碼嗎? 為什麼會看到此訊息?(W)

是(Y) 否(N)

登入及登出

- 在公用電腦使用任何網路服務時，即使瀏覽器關閉，帳戶可能還是會保持在登入狀態。因此，不要忘記在使用結束後，選取 [登出] 來登出您的網路帳戶。
- 如果經常使用公用電腦登入網路服務帳戶，請使用兩個驗證程序功能來協助保護帳戶安全。
- 避免使用不明或無法信任的網路上網，(例如公共場所提供的免費 Wi-Fi) 都要特別小心。避免使用網路銀行或進行網路購物。

鎖定螢幕畫面或裝置

- 如果您要離家一整天，絕對不會忘記關上大門吧？
- 當您不再使用電腦、筆記型電腦或手機時，請一律鎖定螢幕畫面並設定密碼。
- 手機或平板電腦，建議您設定開啟密碼(PIN碼)或透過其他安全模式進行鎖定，以便為您的資料增添多一重的保護。

網路安全必須是一種習慣與文化，而不能只是一種技術與專業。


Thank You!