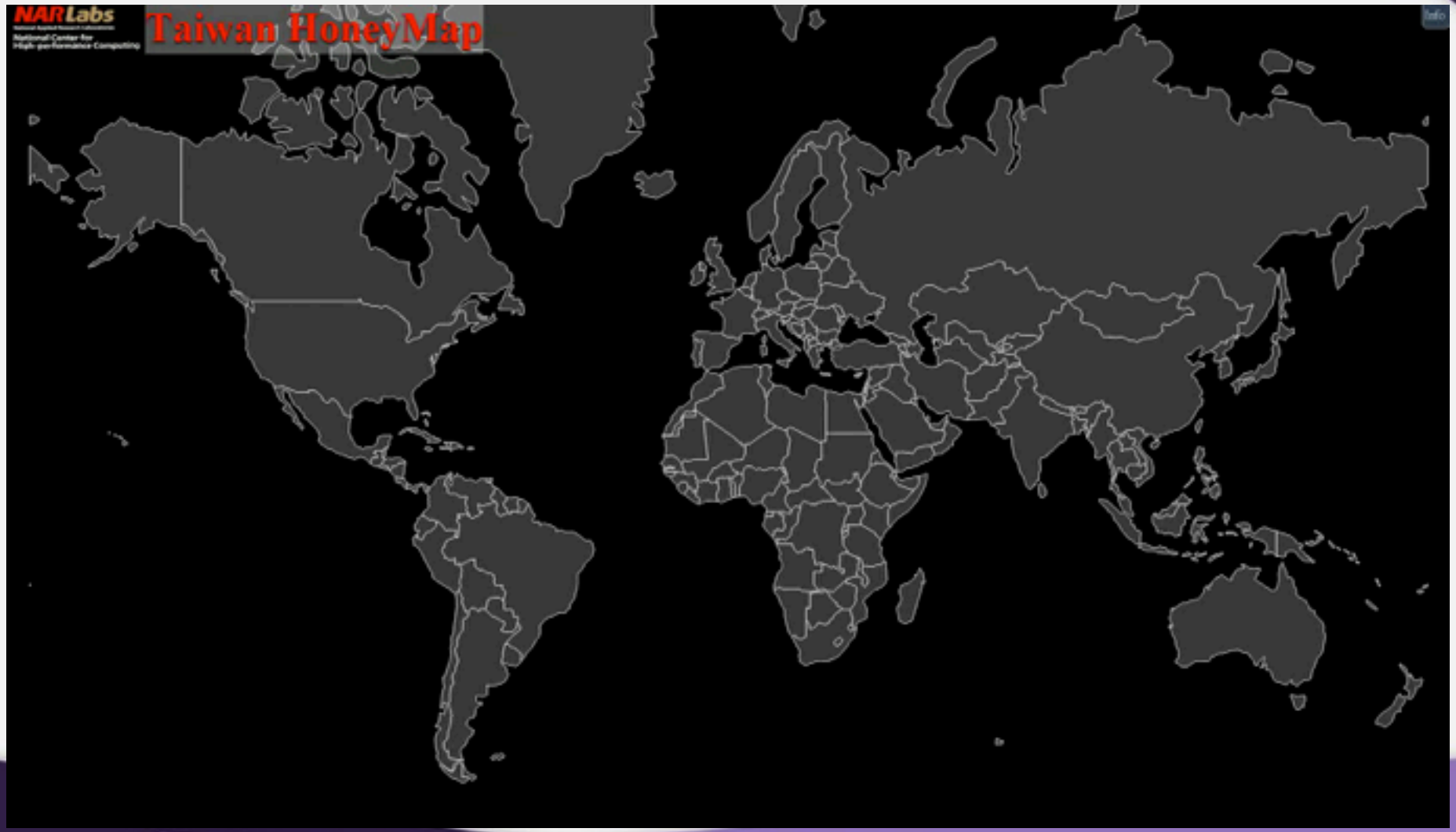
別說我沒跟你說 - 惡意程式即服務的時代來臨

魏宏吉 | 國網中心 佐理研究員

每天不斷重複的發生

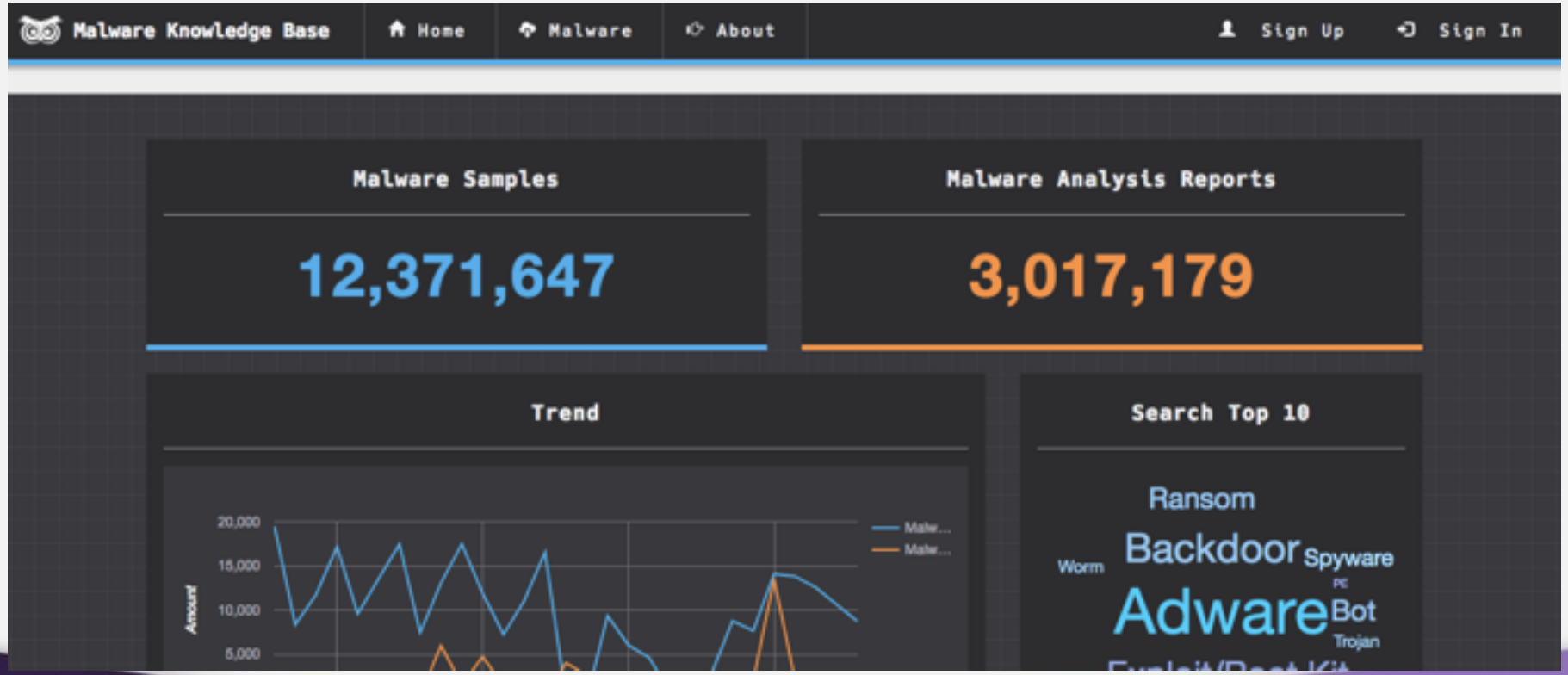
- 每天收集來自學研網路的攻擊日誌、網路流量
- 每天分析來自6,000個IP位址的誘捕日誌
- 每天掌握台灣超過3,000筆的資安事件
- 每天看著CVE編號的成長
- 每天尋著Exploit-Code的實現
- 每天聽著社群網路上的「夢見」與「解夢」
- 每天吸收著來自國際組織的「情資」
- …
- 要做的事好多，但是資安事件還是不斷發生…

惡意程式活動的情況



國網中心惡意程式知識庫

- 提供超過1,237萬隻以上的惡意程式樣本
  - https://owl.nchc.org.tw



ATM設備的惡意程式

新聞

第一銀行ATM疑遭植入惡意程式盜領7000餘萬元，全台400多台ATM停用

第一銀行在上周六、日兩天發生ATM鉅額盜領案，歹徒疑似植入惡意程式，驅動ATM的吐鈔模組，在20家分行34部ATM共盜領7000餘萬元，一銀發現ATM被盜領後，已停止部份的ATM服務，估計全台400多台ATM停止服務。

文/ 蘇文彬 | 2016-07-12 發表

讚 3.8 萬 按讚加入iThome粉絲團 讚 1,313 分享 G+1 1

參考資料：http://www.ithome.com.tw/news/107066

IoT裝置的惡意程式

新聞

駭客公布惡意程式Mirai原始碼，讓數十萬IoT裝置組殭屍網路大軍的元兇現形

惡意程式Mirai可偵測網路上使用出廠預設憑證或固定憑證的物聯網裝置，以植入惡意程式，從遠端操控這些IoT裝置組成殭屍網路，針對特定的對象發動DDoS攻擊，是造成資安部落格KrebsOnSecurity暫時消失的元兇。

文/ 陳曉莉 | 2016-10-03 發表

讚 3.8 萬 按讚加入iThome粉絲團 讚 789 分享 G+1 14

參考資料：http://www.ithome.com.tw/news/108775

惡意程式也需要跨平台

新聞

Windows裝置小心! Mirai木馬程式來了

去年發動數十萬物聯網裝置大軍對資安部落格KrebsOnSecurity進行DDoS攻擊的木馬程式Mirai出現變種版本，資安業者指出該變種版本可感染Windows裝置，擴大了Mirai的威脅性。

文/ 林妍溱 | 2017-02-09 發表

讚 3.8 萬 按讚加入iThome粉絲團 讚 339 分享 G+1 4

參考資料：http://www.ithome.com.tw/news/111854

勒索軟體的來襲

- 勒索軟體(Ransomware)是一種特殊的惡意程式，感染後會加密電腦上的檔案(並非所有檔案)，並要求受害者支付贖金，若選擇不支付贖金，則資料將很可能無法進行解密。

- 不給錢就鎖檔！ 「勒索軟體」 FBI也沒轍
  - https://www.youtube.com/watch?v=FolJeBqox2o

- 付出去的贖金追討的回來嗎?

認識勒索軟體

- 勒索軟體 (Ransomware) 從 2005 年就已出現，剛開始以鎖定螢幕做為勒索手法
- 2013 年開始出現加密型勒索軟體透過郵件附件、網頁惡意廣告等方式入侵電腦後，再用金鑰加密檔案
- 根據加密方式不同，勒索軟體也有不同名稱，如 Crypto L0cker、CryptoWall、CTB Locker 和 Cerber等
- 勒索軟體使用高位元數的金鑰加密

勒索軟體的種類

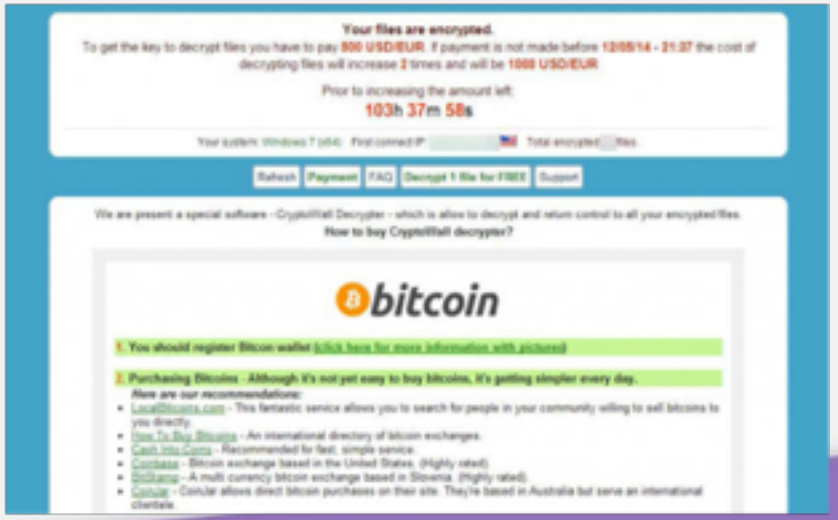
- 限制系統存取類型
  - 使用無法操作系統，鎖住畫面
- 檔案加密類型
  - 針對目標資料夾、檔案使用加密演算法進行處理
  - 主要目標為文件、影音照片等具價值的檔案
- 磁碟加密類型
  - 針對磁碟的MBR與MFT進行加密處理 (例如：PETYA)
  - 開機即看到勒索訊息，無法進行作業系統

各種勒索軟體


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
OK


Payment for private key
MoneyPak
Private key will be destroyed on
10/13/2013
1:23 PM
Time left
71 : 33 : 57
<< Back
Next >>


Your personal files are encrypted by CTB-Locker.
Test decryption.
To make sure that decryption is possible you are allowed to decrypt up to 5 random files for free.
Press 'Search'. Program will scan your disks and decrypt several files.
Press 'Next' to connect to the secret server and decrypt all files.
Press 'Back' to go to the first page.
Search
<< Back
95 : 58 : 28
Next >>


Your files are encrypted.
To get the key to decrypt files you have to pay 500 USD/EUR. If payment is not made before 12/05/14 - 21:37 the cost of decrypting files will increase 2 times and will be 1000 USD/EUR
Prior to increasing the amount left:
103h 37m 58s
Refresh
Payment
FAQ
Decrypt 1 file for FREE
Support
How to buy CryptoWall decrypter?
bitcoin

語音勒索軟體

- Cerber加密勒索軟體具備「語音」能力，用電腦語音來播放，並在俄羅斯地下市場以勒索軟體及服務（RaaS）的形式進行兜售

- 語音的內容如下：
  - 「注意！注意！注意！」「你的文件、照片、資料庫和其他重要檔案都已經被加密！」
  - “Attention! Attention! Attention!”“Your documents, photos, databases and other important files have been encrypted!”

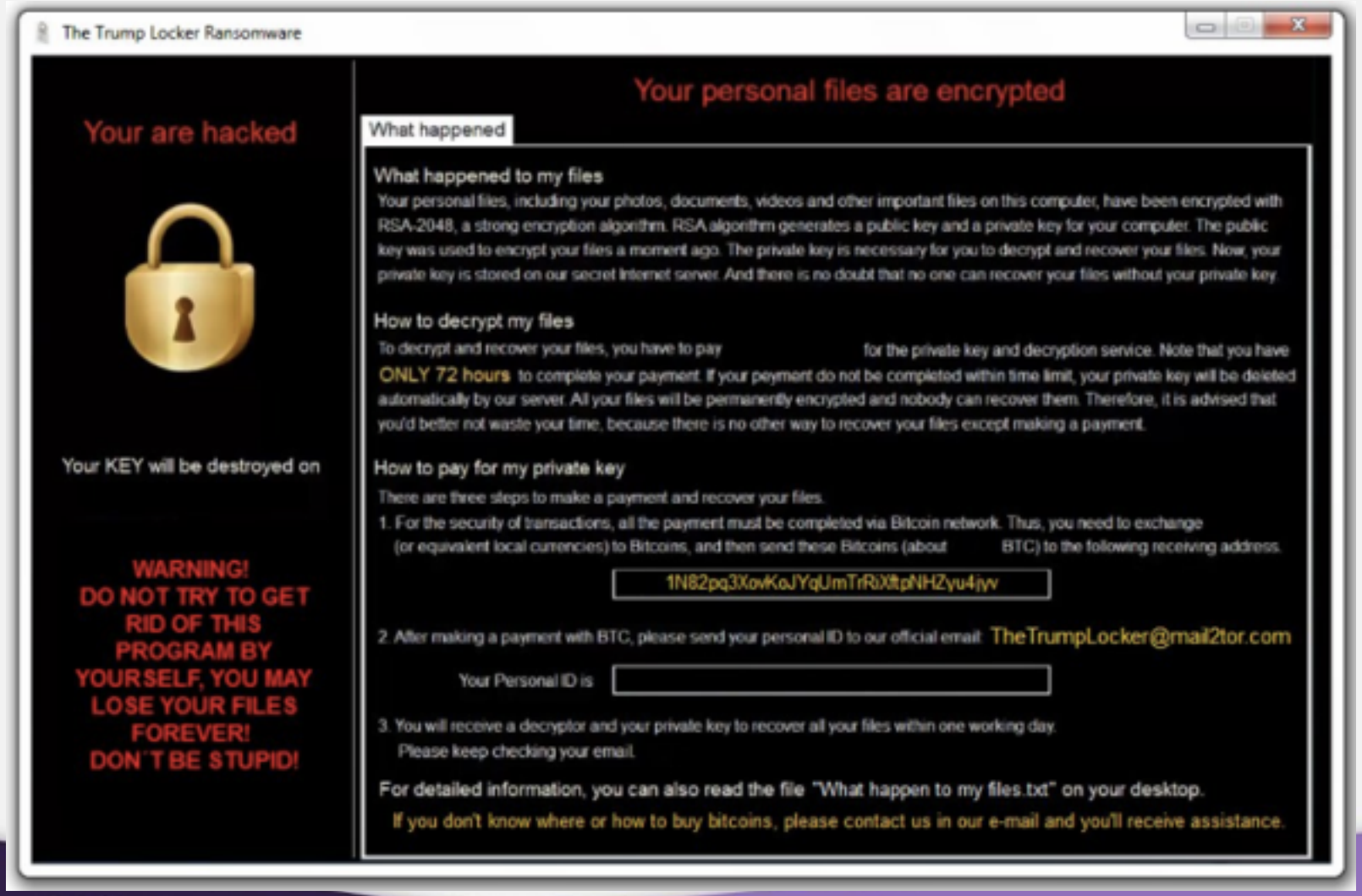
川普來了

- New Trump Locker Ransomware…

Trump Locker temporary splash image

資料來源： https://www.bleepingcomputer.com

不給錢就搗蛋


The Trump Locker Ransomware
Your are hacked
Your KEY will be destroyed on
WARNING!
DO NOT TRY TO GET RID OF THIS PROGRAM BY YOURSELF, YOU MAY LOSE YOUR FILES FOREVER!
DON'T BE STUPID!
Your personal files are encrypted
What happened
What happened to my files
Your personal files, including your photos, documents, videos and other important files on this computer, have been encrypted with RSA-2048, a strong encryption algorithm. RSA algorithm generates a public key and a private key for your computer. The public key was used to encrypt your files a moment ago. The private key is necessary for you to decrypt and recover your files. Now, your private key is stored on our secret Internet server. And there is no doubt that no one can recover your files without your private key.
How to decrypt my files
To decrypt and recover your files, you have to pay for the private key and decryption service. Note that you have ONLY 72 hours to complete your payment. If your peyment do not be completed within time limit, your private key will be deleted automatically by our server. All your files will be permanently encrypted and nobody can recover them. Therefore, it is advised that you'd better not waste your time, because there is no other way to recover your files except making a payment.
How to pay for my private key
There are three steps to make a payment and recover your files.
1. For the security of transactions, all the payment must be completed via Bitcoin network. Thus, you need to exchange (or equivalent local currencies) to Bitcoins, and then send these Bitcoins (about BTC) to the following receiving address.
1N82pq3XovKoJYqUmTrRiXftpNHZyu4jyv
2. After making a payment with BTC, please send your personal ID to our official email: TheTrumpLocker@mail2tor.com
Your Personal ID is
3. You will receive a decryptor and your private key to recover all your files within one working day.
Please keep checking your email.
For detailed information, you can also read the file "What happen to my files.txt" on your desktop.
If you don't know where or how to buy bitcoins, please contact us in our e-mail and you'll receive assistance.

勒索軟體的品質

- 去年三月出現的勒索軟體CryptoMix，因為程式碼品質不佳，許多受害者抱怨支付贖金(5~10 BitCoin)後，還是有些檔案無法被解密

- 駭客並沒有選擇改善CryptoMix的程式碼，而是不斷的變更其名稱，包括CryptFile2、Zeta及最近的CryptoShield

受害者的曙光

新聞

Avast釋出勒索軟體CryptoMix的離線版解密工具

CryptoMix感染了被害者的電腦後，會與C&C伺服器聯繫，建立加密檔案的金鑰，若該電腦無法連網，則在離線下以固定的金鑰加密，Avast釋出所離線版CryptoMix的解密工具。

文/ 陳曉莉 | 2017-02-22 發表

NOT YOUR LANGUAGE? USE https://translate.google.com

What happened to your files ?

All of your files were protected by a strong encryption with RSA-2048.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

How did this happen ?

!!! Specially for your PC was generated personal RSA-2048 KEY, both public and private.
!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.
!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

資料來源： http://www.ithome.com.tw/news/112276

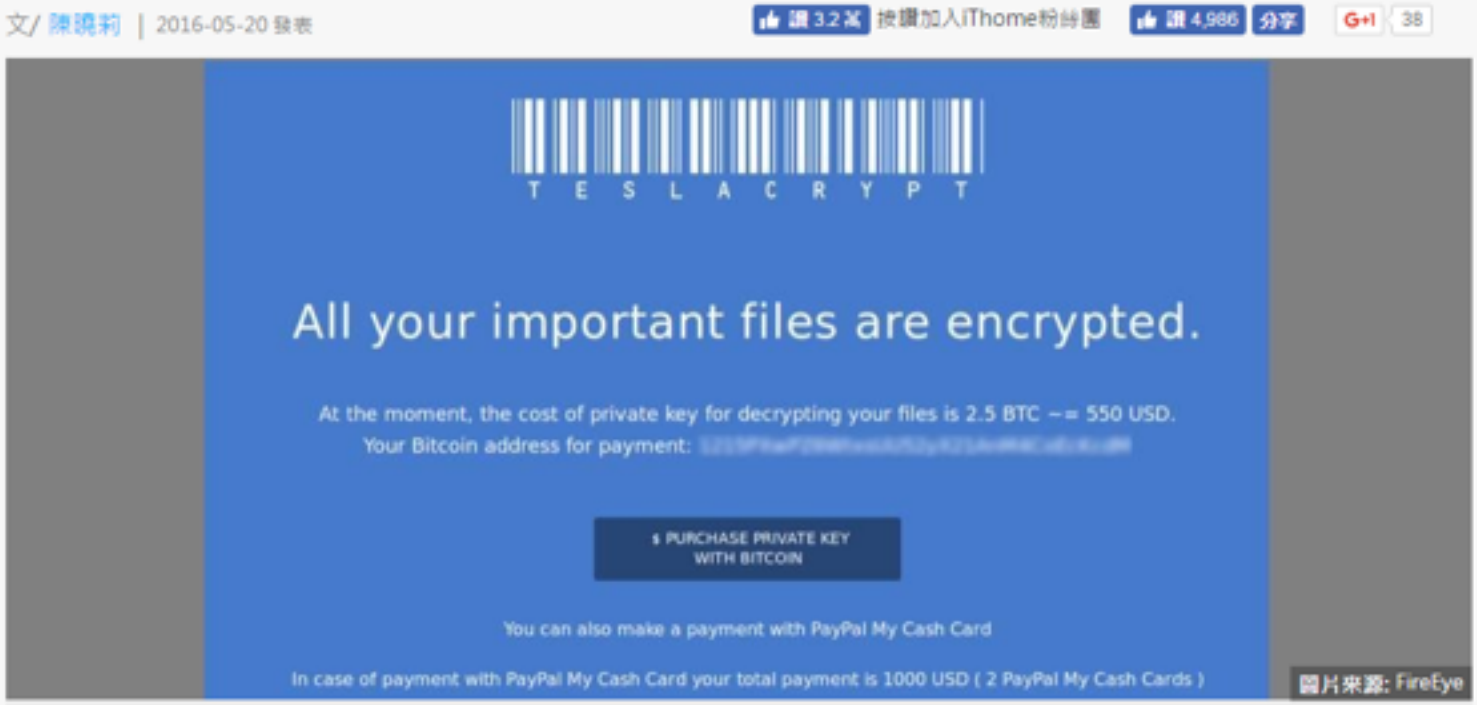
勒索軟體作者的良心

新聞

勒索軟體TeslaCrypt作者良心發現，免費釋出解密金鑰

在2015年2月出現的TeslaCrypt會加密電腦上的系統檔案或遊戲檔案，要求使用者支付贖金。近日其作者似乎良心發現，宣布將結束TeslaCrypt專案，對外道歉，並釋出通用主解密金鑰。

文/ 陳曉莉 | 2016-05-20 發表



TeslaCrypt會加密受害者電腦上的系統檔或遊戲檔，要求使用者付出贖金，估計受害者支付7.6萬美元。

資料來源： http://www.ithome.com.tw/news/106064

無所不賣

資料來源：https://www.youtube.com/watch?v=i4o6M01Hpdc

藍瘦香菇

新聞

WannaCry 2.0勒索蠕蟲狠襲全球，上百個國家受駭，台灣也是重災區

週五開始出現全球性攻擊，到了週六，災情更從十幾個國家迅速擴大到104個國家，攻擊次數擴大到12.6萬次，儘管全球都是受災區，但WCry的主要攻擊目標為俄國、烏克蘭與台灣

文/ 陳曉莉 | 2017-05-14 發表

讚 4.1 萬 按讚加入iThome粉絲團 讚 255 分享 G+1 1

資料來源： http://www.ithome.com.tw/news/114144

WannaCry勒索軟體來自？

一波未平一波又起

資料來源： http://www.ithome.com.tw/news/112276

防護建議

- 更新作業系統 (必要)
- 限制或關閉 Port 445存取 (必要)
- 更改使用複雜的密碼 (必要)
- 製作Kill-Switch (暫時)
- 安裝MBRFilter (急用)
- 關閉WMI服務 (急用)

資料來源： http://www.ithome.com.tw/news/112276

做好備份才是王道

- 最佳備份實作規則是三二一原則
  - 至少備份三份
  - 使用二種不同形式
  - 其中一份備份要存放異地

問題與討論