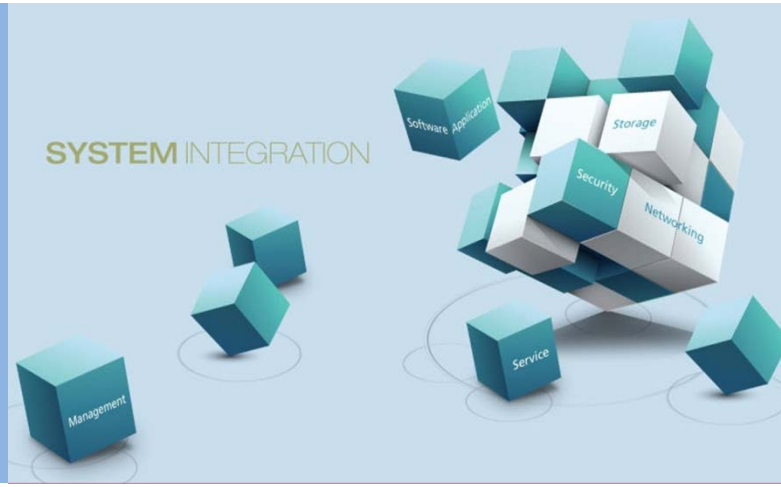
麟 瑞 科 技
RING LINE CORPORATION

勒贖軟體強勢再進化
銷售支援部-資安組



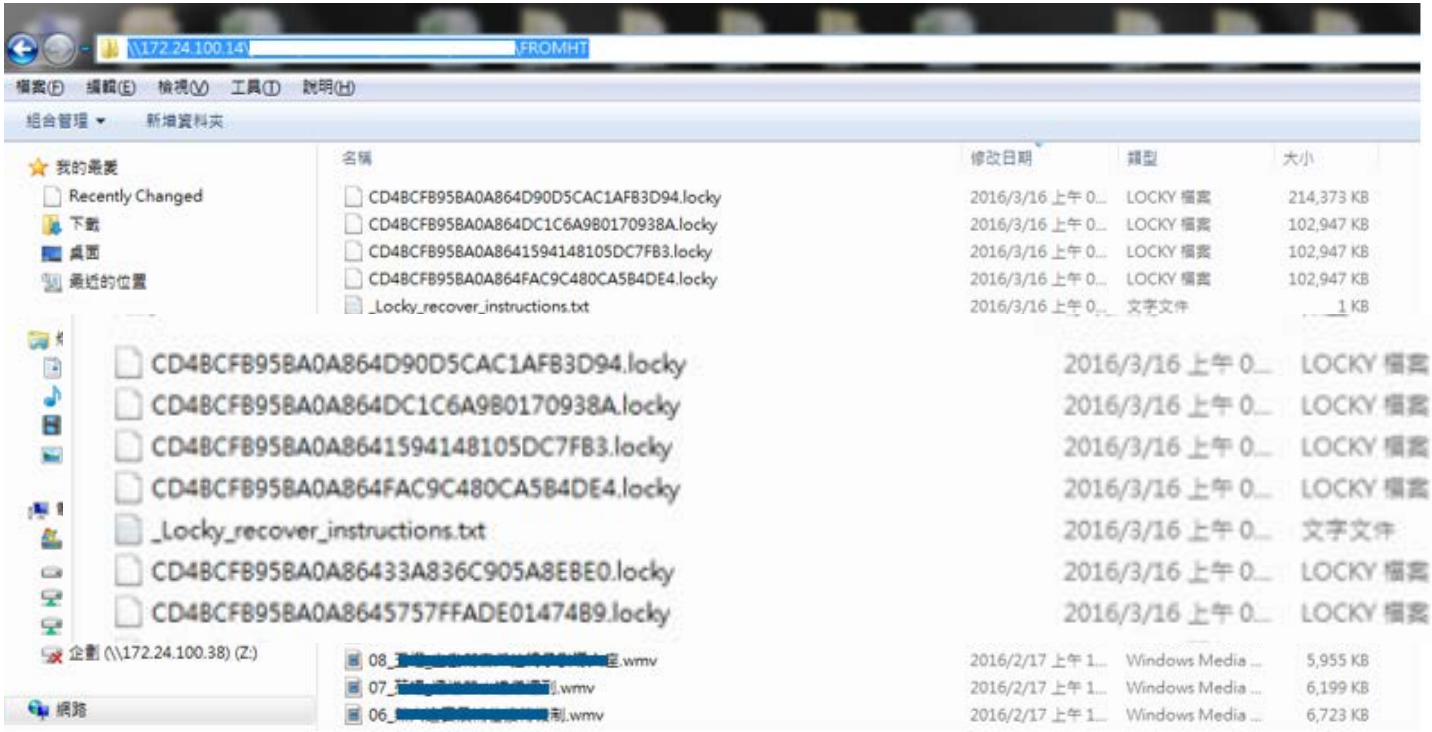
Brian Hu

VCP、NAASAP、CCNP、CEH、
ISO27001 LA

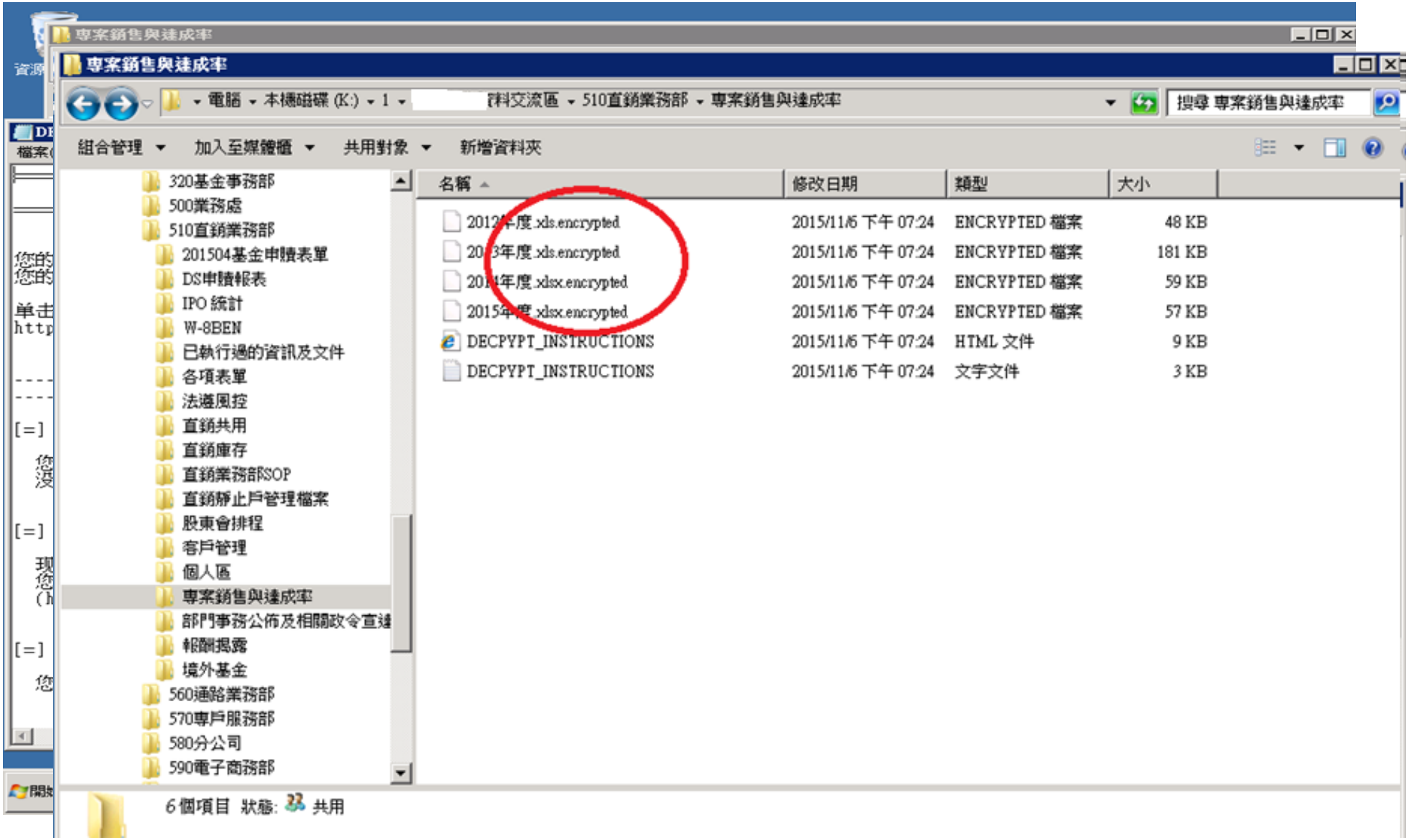
簡報大綱

- 勒索軟體大災問
- 勒贖病毒感染行為與特徵介紹
- 勒贖病毒防禦介紹
- 勒贖病毒案例
- Q & A

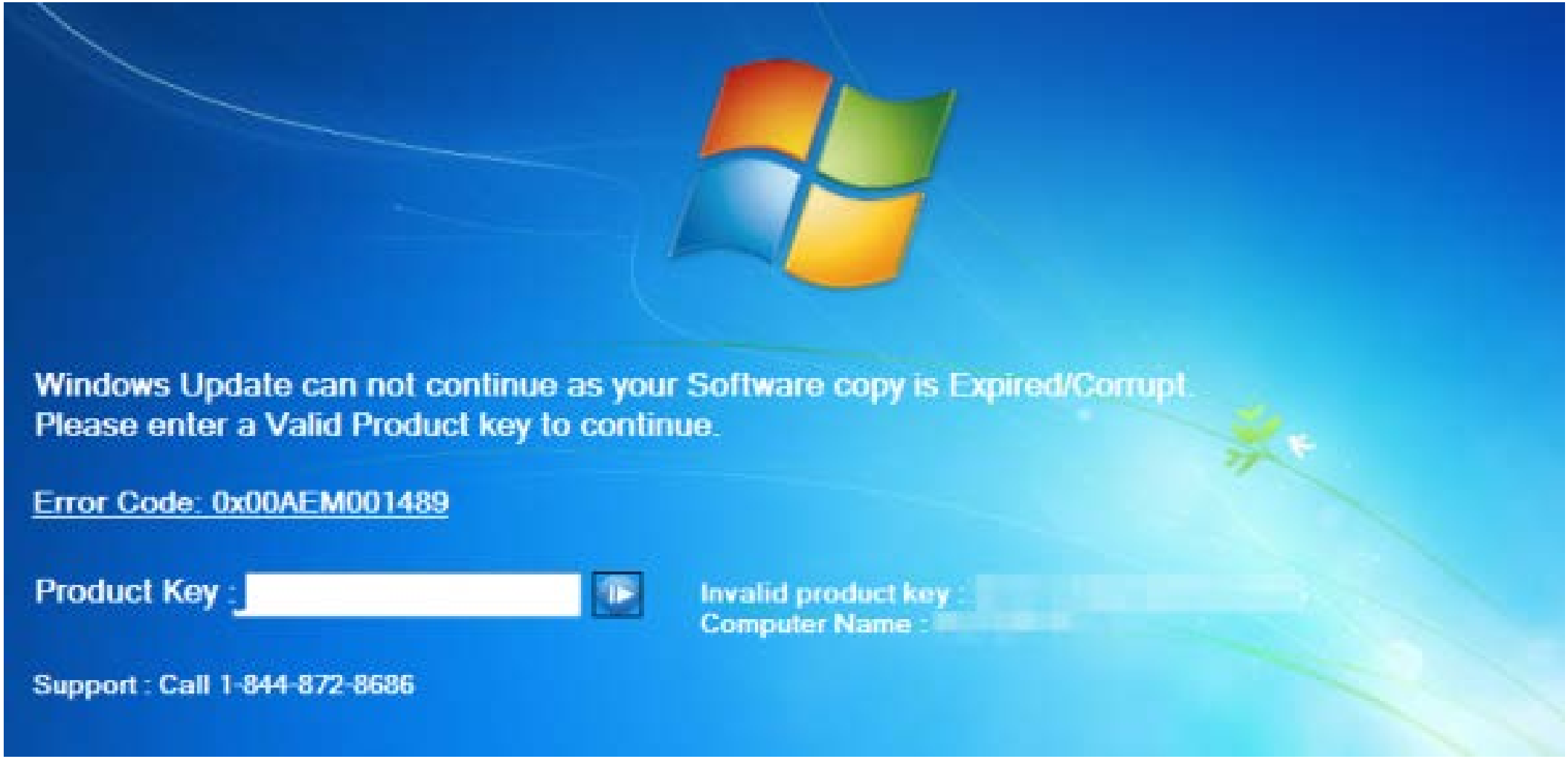
今天locky了嗎?


\\172.24.100.14\ \FROMHT
檔案(F) 編輯(E) 檢視(V) 工具(T) 說明(H)
組合管理 新增資料夾
我的最愛
Recently Changed
下載
桌面
最近的位置
名稱 修改日期 類型 大小
CD4BCFB95BA0A864D90D5CAC1AFB3D94.locky 2016/3/16 上午 0... LOCKY 檔案 214,373 KB
CD4BCFB95BA0A864DC1C6A980170938A.locky 2016/3/16 上午 0... LOCKY 檔案 102,947 KB
CD4BCFB95BA0A8641594148105DC7FB3.locky 2016/3/16 上午 0... LOCKY 檔案 102,947 KB
CD4BCFB95BA0A864FAC9C480CA5B4DE4.locky 2016/3/16 上午 0... LOCKY 檔案 102,947 KB
_Locky_recover_instructions.txt 2016/3/16 上午 0... 文字文件 1 KB
CD4BCFB95BA0A86433A836C905A8EBE0.locky 2016/3/16 上午 0... LOCKY 檔案 5,516 KB
CD4BCFB95BA0A8645757FFADE01474B9.locky 2016/3/16 上午 0... LOCKY 檔案 5,516 KB
企劃 (\\172.24.100.38) (Z:)
網路
08_ .wmv 2016/2/17 上午 1... Windows Media ... 5,955 KB
07_ .wmv 2016/2/17 上午 1... Windows Media ... 6,199 KB
06_ .wmv 2016/2/17 上午 1... Windows Media ... 6,723 KB

恭喜你!!中獎了


專案銷售與達成率
專案銷售與達成率
電腦 ▸ 本機磁碟 (K:) ▸ 1 ▸ 資料交流區 ▸ 510直銷業務部 ▸ 專案銷售與達成率
搜尋 專案銷售與達成率
組合管理
加入至媒體櫃
共用對象
新增資料夾
320基金事務部
500業務處
510直銷業務部
201504基金申購表單
DS申購報表
IPO 統計
W-8BEN
已執行過的資訊及文件
各項表單
法遵風控
直銷共用
直銷庫存
直銷業務部SOP
直銷靜止戶管理檔案
股東會排程
客戶管理
個人區
專案銷售與達成率
部門事務公佈及相關政令宣達
報酬揭露
境外基金
560通路業務部
570專戶服務部
580分公司
590電子商務部
名稱
修改日期
類型
大小
2012年度.xls.encrypted 2015/11/6 下午 07:24 ENCRYPTED 檔案 48 KB
2013年度.xls.encrypted 2015/11/6 下午 07:24 ENCRYPTED 檔案 181 KB
2014年度.xlsx.encrypted 2015/11/6 下午 07:24 ENCRYPTED 檔案 59 KB
2015年度.xlsx.encrypted 2015/11/6 下午 07:24 ENCRYPTED 檔案 57 KB
DECPYPT_INSTRUCTIONS 2015/11/6 下午 07:24 HTML 文件 9 KB
DECPYPT_INSTRUCTIONS 2015/11/6 下午 07:24 文字文件 3 KB
6 個項目 狀態: 共用

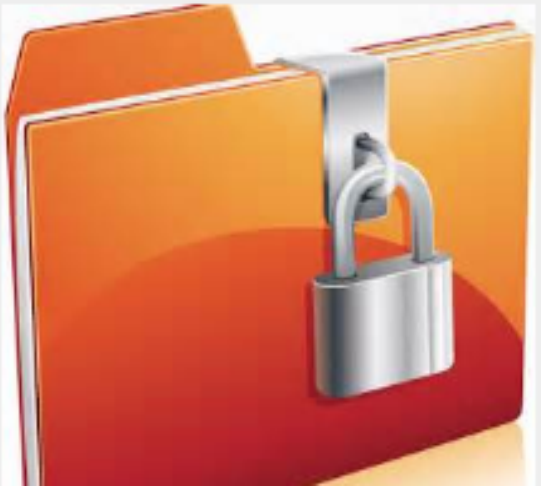
勒索軟件迫受害人交「服務費」解鎖



什麼是勒索病毒

什麼是勒索病毒

- 勒索病毒會綁架電腦裡面檔案作為『人質』，要求被駭者付出『贖金』以贖回電腦裡面已經被加密檔案
- 針對使用者的檔案(包含：Office, PDF, 圖片, 影音檔...等)進行最高等級的加密(RSA 2048 bit)，讓使用者無法開啟加密後的檔案，進而達成勒索使用者付100元美金或是比特幣等方式。
- 由於解密金鑰在駭客手上，若沒有付贖金則無法取得解密金鑰，也就是無法還原檔案。



可否透過逆向技術解密檔案?

中了勒索軟體該怎麼辦?能不能救回來

付錢消災！電腦勒索病毒 FBI也沒轍

分享 | G+ 分享 | 留言 | 列印 | 存新聞 | A- A+

2015-12-01 18:34 台灣醒報 記者鄭國強／台北報導 讚 分享 391 G+1 1

實在恐怖，看到「.pdf」檔案點進去，竟然就中了勒索病毒cryptowall，它不但偽裝成別的檔案類型，還會將你的檔案加密，若要救回就必須付出高額比特幣。如今，就連美國聯邦調查局FBI也束手無策。防毒軟體卡巴斯基工程師表示，目前防毒軟體可以防毒、清理掉病毒，但無法對被加密的檔案解密，刑事局表示，知道此類軟體存在，但未接獲任何報案。

贖回須付彼特幣

這種附加檔名會偽裝成「.pdf」、「.exe」的勒索病毒自2013年起源自俄羅斯，有CryptoLocker、Cryptowall、Torrentlocker等主要幾種病毒，它們會將使用者的檔案加密，若要救回，請付錢解密。負責監督FBI網路安全與電腦情資的助理探員約瑟夫，10月底在一場波士頓的演講上表示，若個人中了勒索電腦病毒，最快的解救方式就是付錢贖回檔案。

資料來源：聯合新聞網

沒有備份只能花錢消災

如果沒有備份的情況下

中了勒索軟體該怎麼辦？FBI回答：解密資料的最快方法就是花錢消災！

美國FBI探員Joseph Bonavolonta近日在波士頓舉行的網路安全高峰會上表示，雖然鼓勵受害者向FBI報案，但FBI無法替受害者取回加密的資料，最簡單的方式就是支付贖金。還說勒索軟體賺很多錢的原因就是絕大多數的人都選擇了支付贖金，而且可能因為這樣，駭客也不會要求太高的贖金，同時也會履行承諾幫受害者解密。

文/ 陳曉莉 | 2015-10-28 發表

讚 2.1萬 按讚加入iThome粉絲團 讚 分享 1,187 G+1 19

iThome 電腦報 Weekly
按讚追蹤 iThome 最新報導
讚 2.1萬

熱門新聞

微軟在北美開賣容量高達1TB的Surface Book與Surface Pro 4
2016-01-25

張善政接任過渡內閣閣揆，與新政府打造交接典範，強調資安無縫接軌
2016-01-26

專家觀點：Docker架構優缺

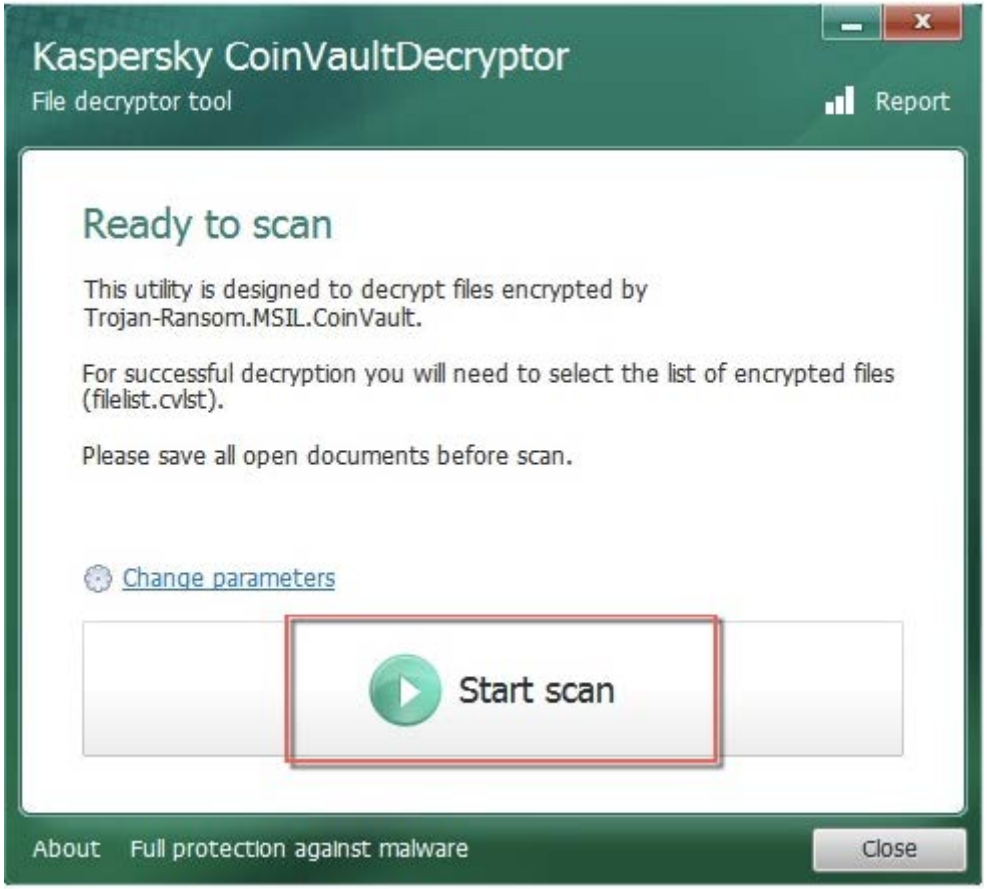
真的沒的救嗎?試試解密工具

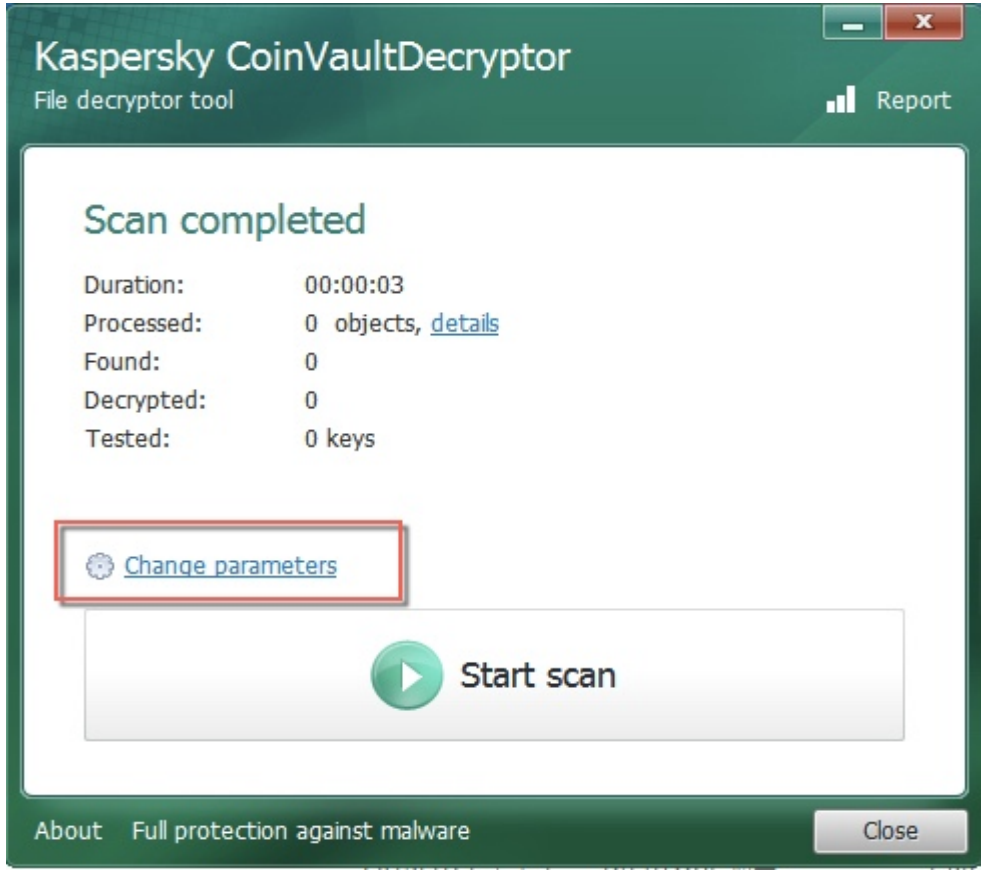
已經有廠商提供解密工具

CoinVault
Bitcryptor
TeslaCrypt
Linux.Encoder.1
CryptoLocker

Kaspersky CoinVaultDecryptor

- 不保證100%有效，





勒索軟件TeslaCrypt於心有愧！

http://www.pc3mag.com/teslacrypt-solve/

受害後的應變之道：

1. 立即切斷網路連線，並關機避免繼續加密未完成的檔案，將硬碟拆下至另一台電腦備份其資料
2. 重灌電腦
3. 還原已備份檔案
4. 付贖金

SYSTEM INTEGRATION Software Application Storage

簡報大綱

- 勒索軟體大災問
- 勒贖病毒感染行為與特徵介紹
- 勒贖病毒防禦介紹
- 勒贖病毒案例
- Demo 與 Q & A

勒索軟體新聞事件(行為特徵)

現階段，大多數的加密勒索軟體都是透過釣魚郵件入侵，若使用者風險意識不夠，就很可能受害，導致檔案無法存取。

從大多數的加密勒索病毒的執行過程來看，一般都是會向遠端遙控C&C主機取得加密金鑰，再暗中加密受害電腦中的檔案，像是先使用AES加密檔案，再用非對稱金鑰RSA加密來將AES金鑰加密，且金鑰長度是2048位元，使用戶難以用暴力方式解開加密，因為即便用超級電腦，都要運算個好幾年才能達到目的。

當用戶電腦中的重要檔案，像是Word、Excel、PowerPoint、PDF、JPG檔，等近百種常見檔案格式，都被惡意加密後。加密勒索病毒就會跳出要求付贖金的勒索訊息，並限期在很短時間內（像是3天）就要給付，否則銷毀金鑰，讓用戶再也無法解開檔案。同時，勒索給付方式上，為了更隱匿蹤跡，會要求以比特幣等金流機制來給付，才能取得解密金鑰。

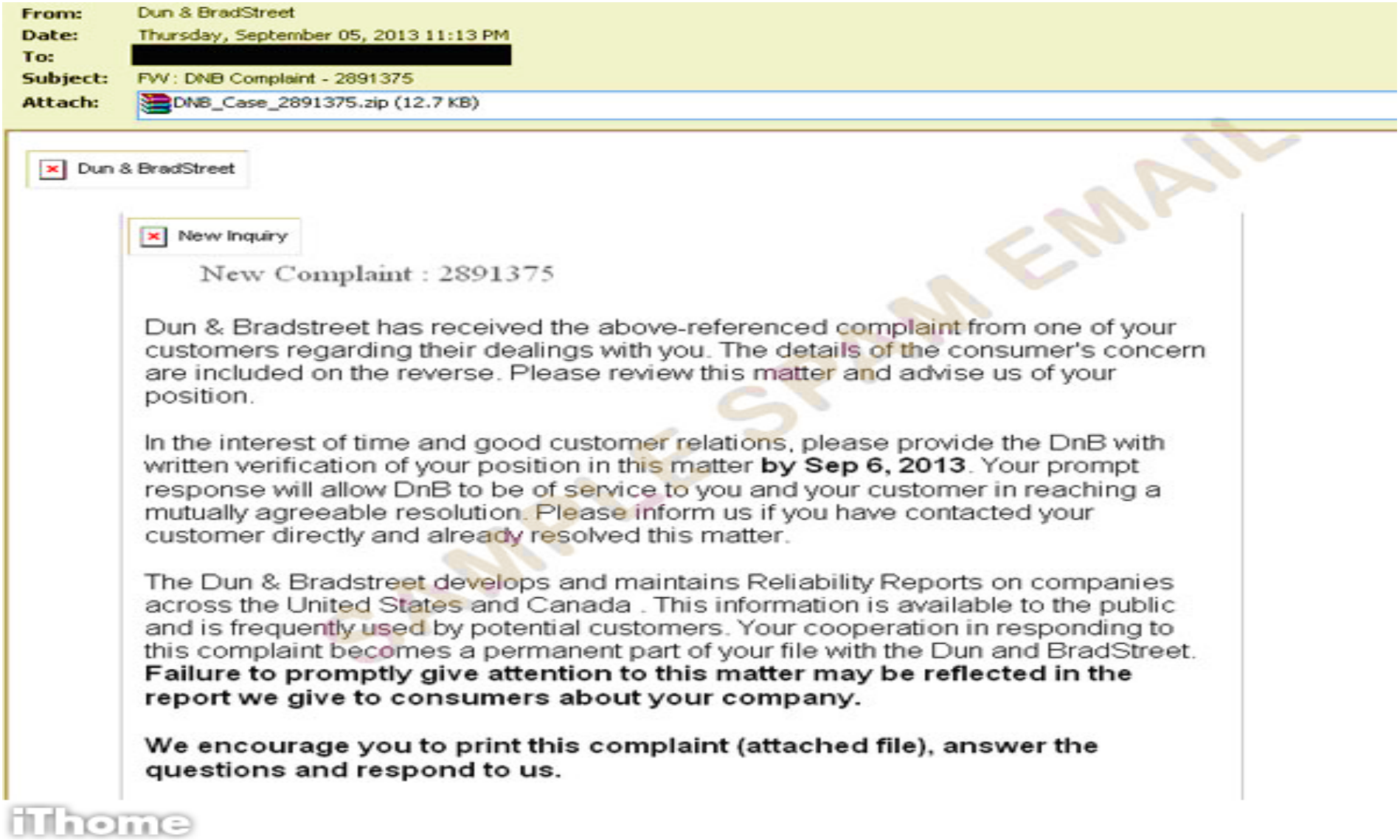
勒索軟體新聞事件(滲透管道)

史上最狠的勒索軟體CryptoLocker從9月開始在全球各地肆虐，臺灣企業也成了攻擊標的，陸續傳出受災消息。

CryptoLocker透過釣魚郵件入侵，鎖定受害者電腦中、USB、網路芳鄰、雲端硬碟、檔案伺服器的檔案，駭客混用AES與RSA這2種加密技術，將檔案全數加密，導致檔案無法存取，受害者想要自行復原，簡直是天方夜譚。駭客並且限期3天（另有一說，限期４天）內，必須支付3,000或9,000元贖金，否則將毀損解密金鑰，代表受害者針對的檔案將會全數消失。

CryptoLocker雖然會搜尋所有網路上的檔案，但並不會透過內網散播，也就是說，假設企業內僅一臺電腦受害，其他使用者只要不被社交工程誘騙成功，就不會有感染的可能。Sophos臺灣區技術經理詹鴻基表示，這個軟體主要會對本機電腦裡面以及網路硬碟中的特定目標檔案類型進行加密，除此之外沒有其他的破壞行為。

社交工程信件散播(滲透管道)



From: Dun & BradStreet
Date: Thursday, September 05, 2013 11:13 PM
To: [redacted]
Subject: FW: DNB Complaint - 2891375
Attach: DNB_Case_2891375.zip (12.7 KB)

Dun & BradStreet

New Inquiry

New Complaint : 2891375

Dun & Bradstreet has received the above-referenced complaint from one of your customers regarding their dealings with you. The details of the consumer's concern are included on the reverse. Please review this matter and advise us of your position.

In the interest of time and good customer relations, please provide the DnB with written verification of your position in this matter **by Sep 6, 2013**. Your prompt response will allow DnB to be of service to you and your customer in reaching a mutually agreeable resolution. Please inform us if you have contacted your customer directly and already resolved this matter.

The Dun & Bradstreet develops and maintains Reliability Reports on companies across the United States and Canada . This information is available to the public and is frequently used by potential customers. Your cooperation in responding to this complaint becomes a permanent part of your file with the Dun and BradStreet. **Failure to promptly give attention to this matter may be reflected in the report we give to consumers about your company.**

We encourage you to print this complaint (attached file), answer the questions and respond to us.

SPAM EMAIL
iThome

惡意廣告(滲透管道)

Thank You
November 18
祝賀您
您已經被選中 參加我們的年度訪客意見調查。這將只需要您30秒的時間，它將幫助我們增強用
戶體驗。完成後，您將有機會獲得一台 HTC One®, iPhone 6®, 或一台 Samsung Galaxy S5®.
現在開始 ›

勒索軟體新聞事件(滲透管道)

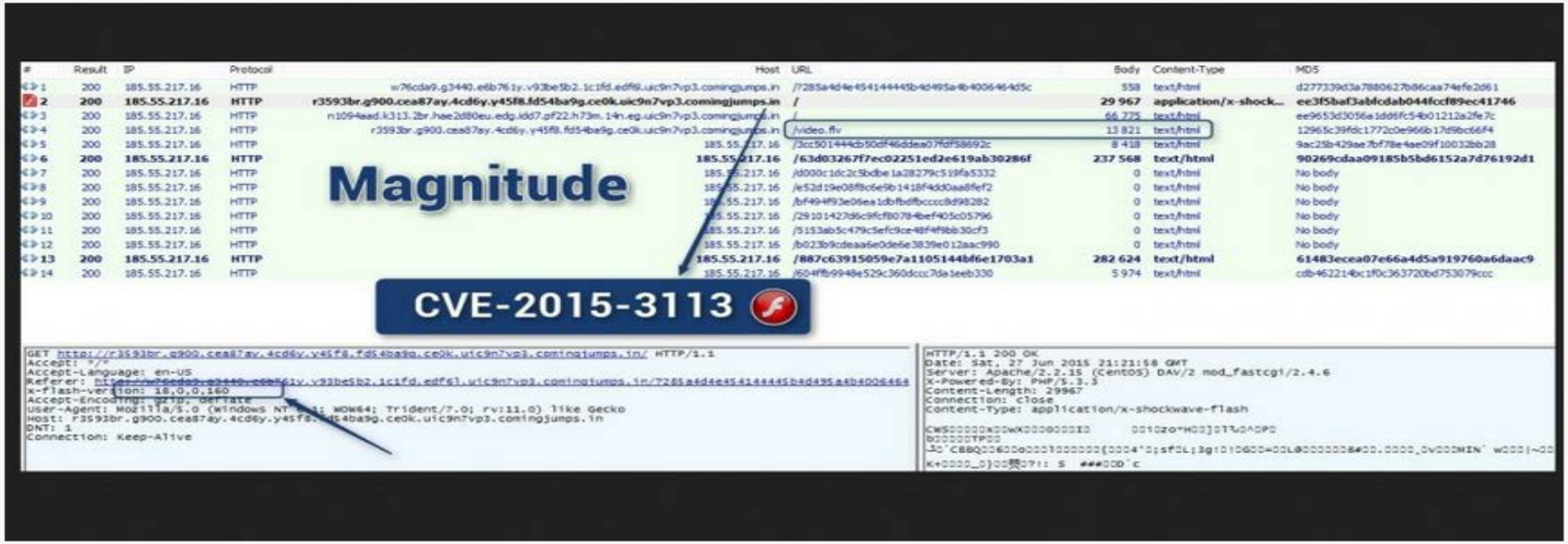
新聞

知名攻擊套件已鎖定才剛修補的Flash零時差漏洞，專門安裝勒索軟體

資安業者Trustwave估計Magnitude在攻擊程式套件市場擁有31%的佔有率，並與駭客拆分攻擊收益，安全研究人員Kafeine則指出，Magnitude漏洞攻擊程式已納入最新的Flash漏洞進行攻擊，以安裝Cryptowall勒索軟體。

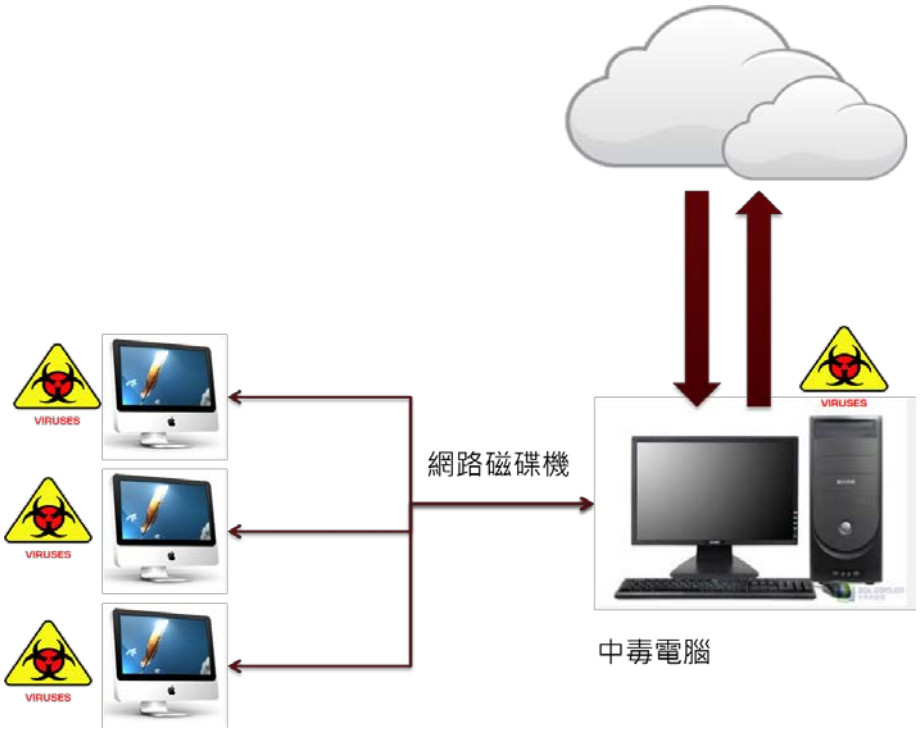
文/ 陳曉莉 | 2015-07-01 發表

讚 1.4 萬 按讚加入iThome粉絲團 讚 分享 862 g+1 44



主要來自二個管道

- 電子郵件
  - 文件檔案
  - 執行檔案
  - 腳本檔案(JS)
- 網際網路
  - 釣魚網站



感染途徑-網頁釣魚郵件

大部分收到勒索軟體入侵的原因都是誤點了網路釣魚郵件，網路釣魚郵件內容可區分以下幾種類型:

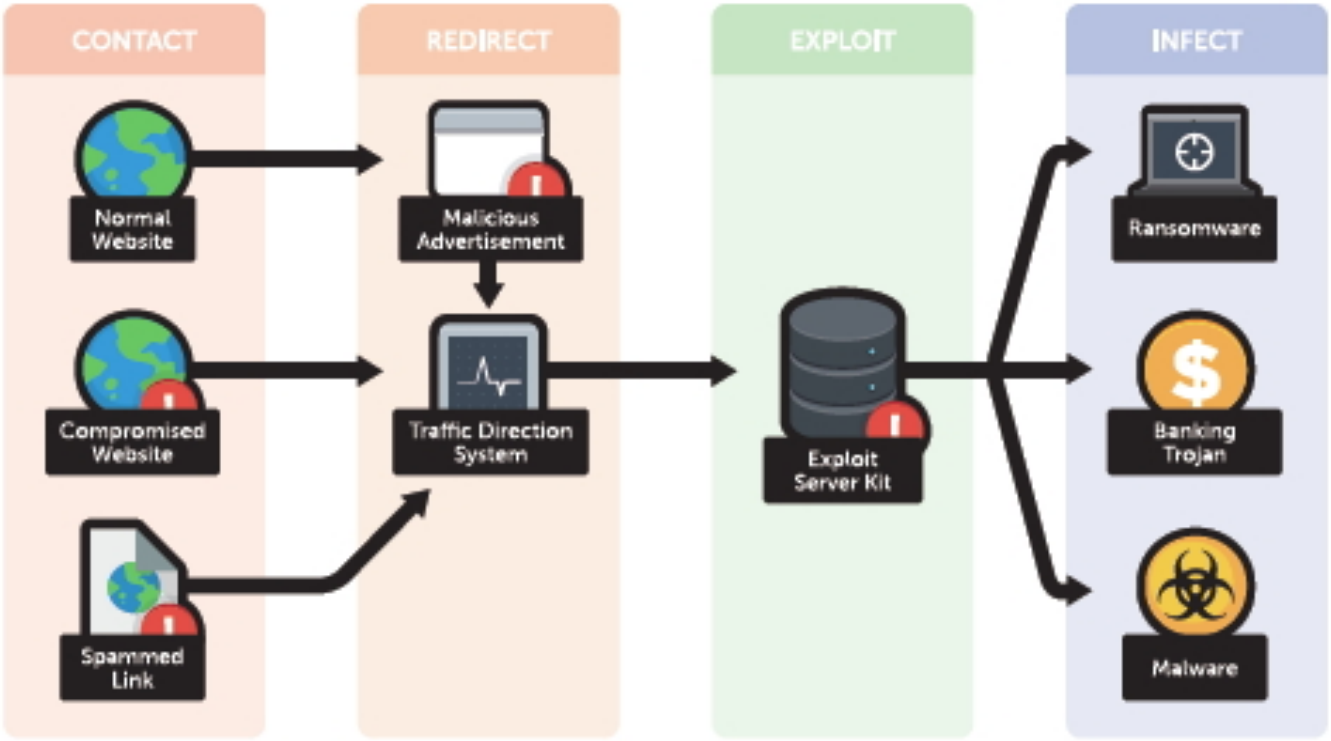
1. 快遞或郵寄通知
2. 帳單或訂單
3. 應徵者履歷
4. 退稅、發票或罰單

感染途徑-惡意廣告Pre-Click

感染途徑-惡意廣告Post-Click

感染途徑-網頁掛馬

勒索軟體會透過入侵網路來達到散步勒索軟體的目的，當發現網站伺服器或應用程式有漏洞時，便會入侵並在網頁上置入Script導向裝載「漏洞攻擊套件」(即常說的Exploit Kit)的網頁，此時此套件便會掃描使用者漏洞來達到主動下載且執行勒索軟體。



Exploit kit的攻擊流程

勒索軟體總結

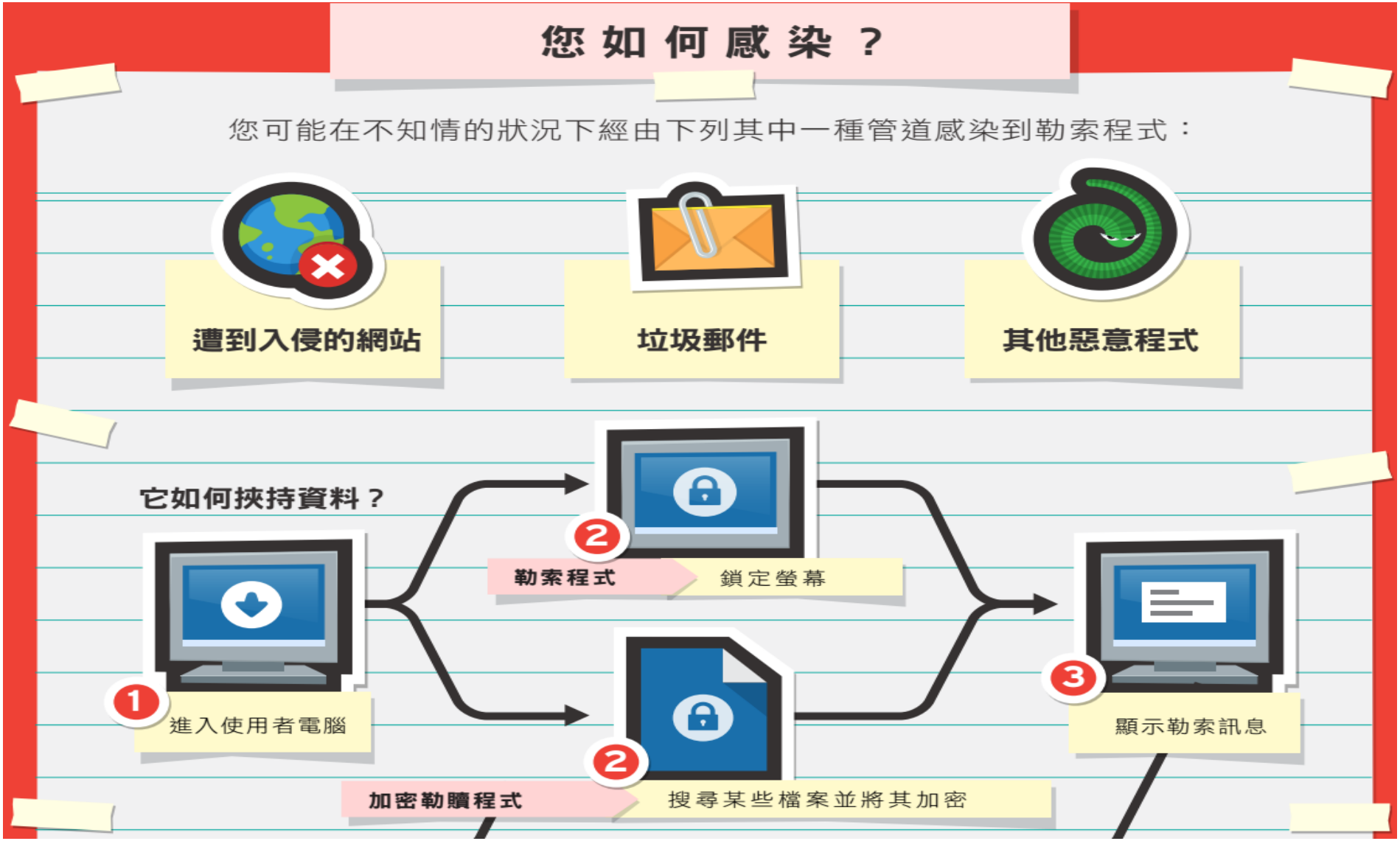
勒索程式

定義、原理和後果

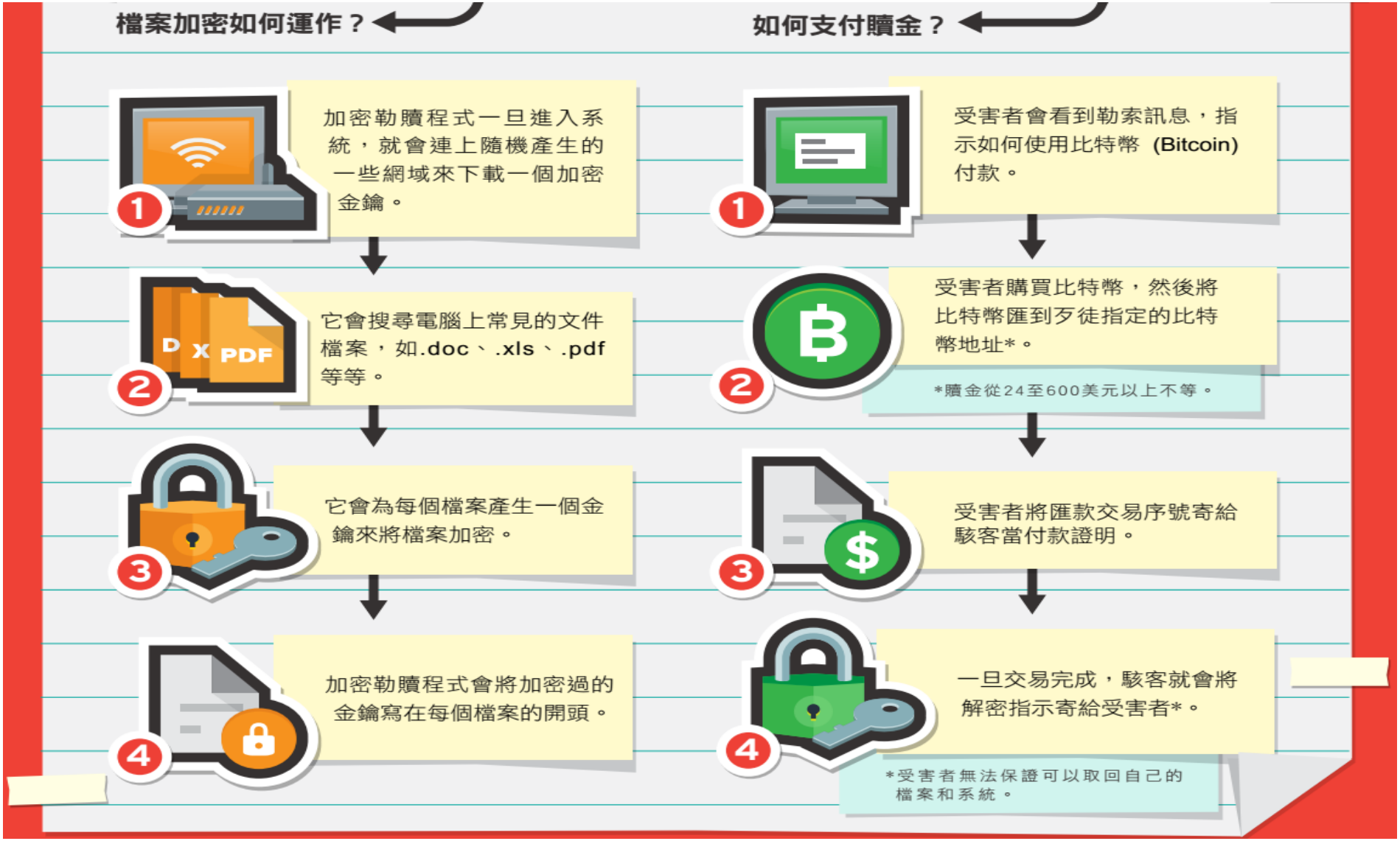
什麼是勒索程式？

勒索程式是一種會挾持資料的嚴重資安威脅，它會讓檔案和系統功能無法使用，甚至讓整台電腦都無法使用。受害者必須支付一筆贖金來贖回自己的檔案和系統。

感染方式


您 如 何 感 染 ？
您可能在不知情的狀況下經由下列其中一種管道感染到勒索程式：
遭到入侵的網站
垃圾郵件
其他惡意程式
它如何挾持資料？
1
進入使用者電腦
2
勒索程式
鎖定螢幕
2
加密勒贖程式
搜尋某些檔案並將其加密
3
顯示勒索訊息

行為運作

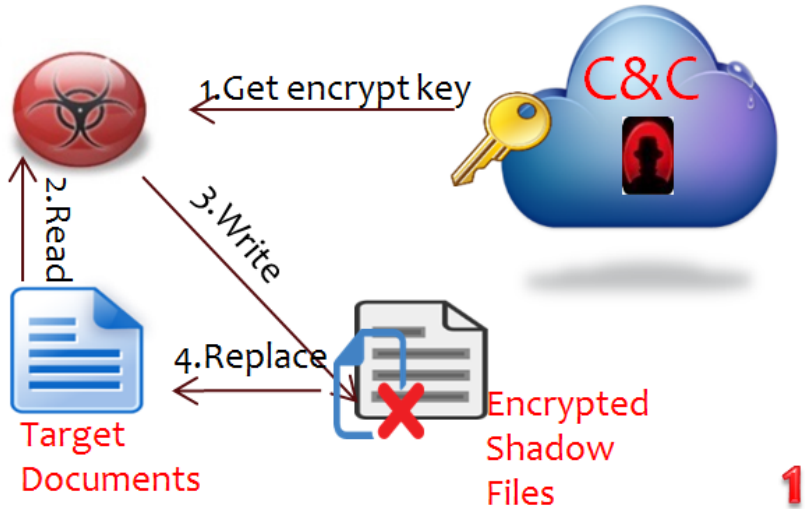

檔案加密如何運作？
加密勒贖程式一旦進入系統，就會連上隨機產生的一些網域來下載一個加密金鑰。
它會搜尋電腦上常見的文件檔案，如.doc、.xls、.pdf等等。
D X PDF
它會為每個檔案產生一個金鑰來將檔案加密。
加密勒贖程式會將加密過的金鑰寫在每個檔案的開頭。
如何支付贖金？
受害者會看到勒索訊息，指示如何使用比特幣 (Bitcoin)付款。
受害者購買比特幣，然後將比特幣匯到歹徒指定的比特幣地址*。
*贖金從24至600美元以上不等。
受害者將匯款交易序號寄給駭客當付款證明。
一旦交易完成，駭客就會將解密指示寄給受害者*。
*受害者無法保證可以取回自己的檔案和系統。

被感染的電腦會..

- 加密電腦中“有寫入權限“文件檔案
- 加密包含所有網路磁碟機的文件檔案
- 加密完成後顯示如何
  取得解密的方法!!

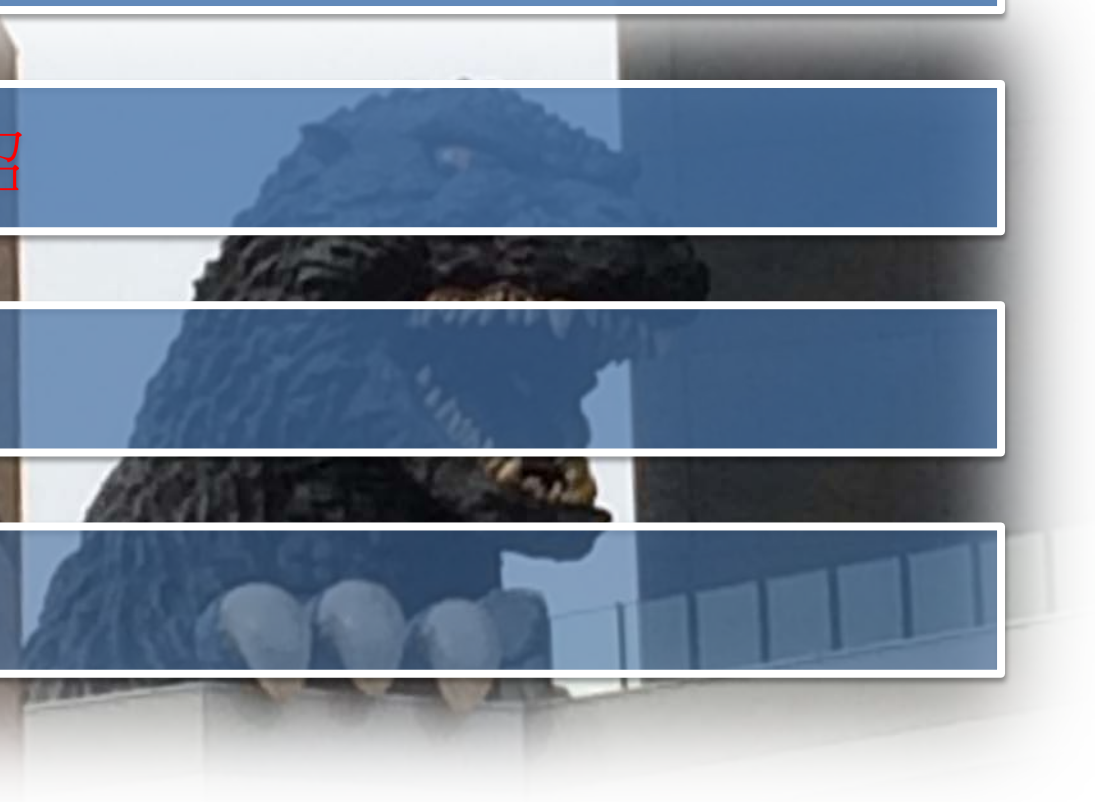
被加密後能否自行解開?

- 檔案是由AES / RSA 2048 加密演算法加密
- 一經加密即無法破解, 除非取得金鑰



簡報大綱

- 勒索軟體大災問
- 勒贖病毒感染行為與特徵介紹
- 勒贖病毒防護介紹
- 勒贖病毒事件簿
- Q & A



個人如何防護

您如何保護自己？

感染勒索程式目前還沒有解藥，不過使用者可以藉由下列方法來防止自己感染：

定期備份資料

遵守 3-2-1 原則：3 份備份、2 種儲存媒體、1 個不同的安全存放地點。

將網站加入書籤

將您經常瀏覽及信任的網站加入書籤當中，可防止您意外打錯網址的風險。

檢查電子郵件來源

在開啟任何電子郵件中的連結或下載其中的檔案之前，務必先仔細核對寄件人的地址是否在您的通訊錄當中。

更新您的防護軟體

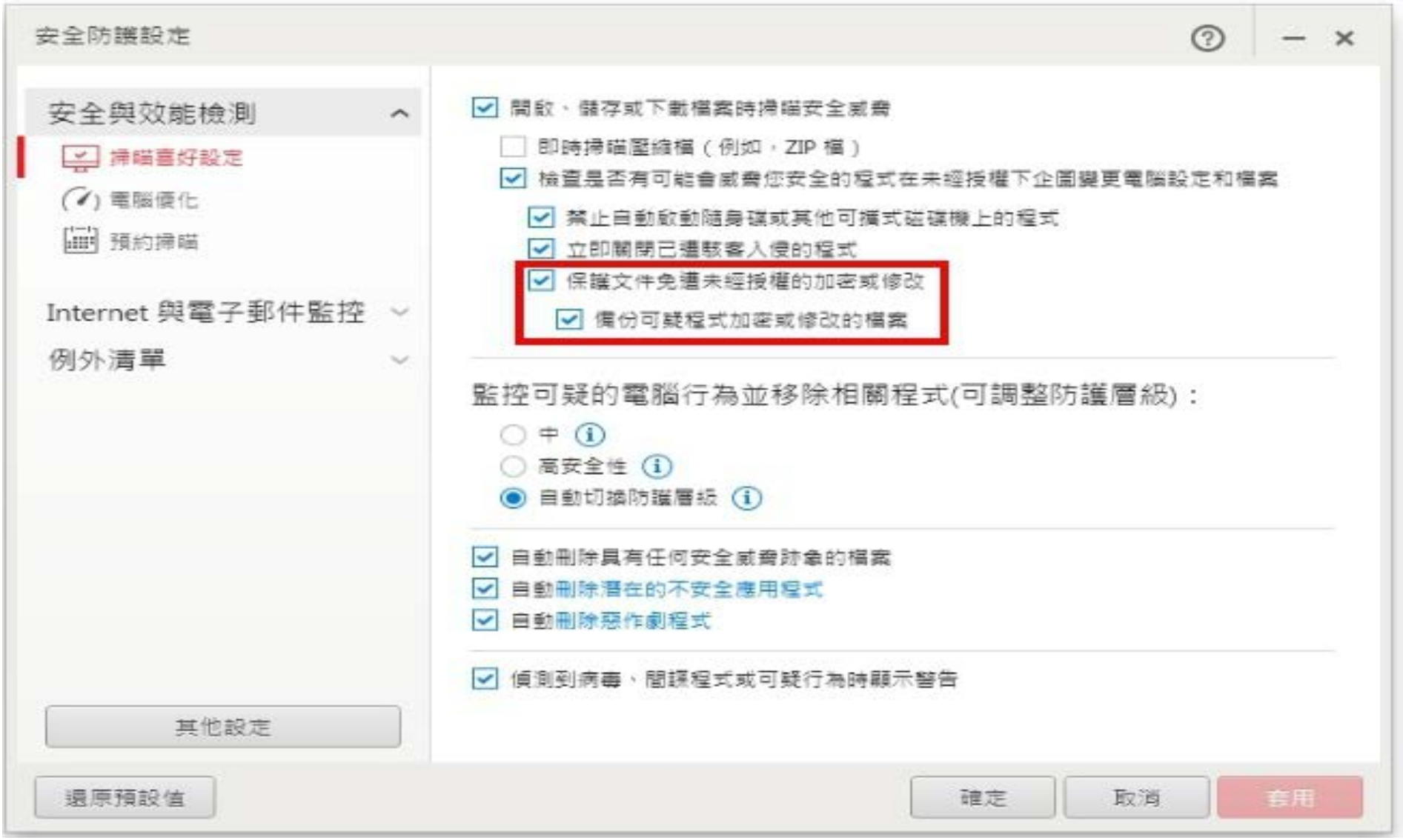
保持最新狀態的防護軟體可讓您多一層保障，因此請務必定期更新，讓您有防範最新勒索程式變種的能力。

卡巴斯基

如往常一樣，卡巴斯基安全專家並不建議受害人為了個人金錢而支付贖金，因為這樣會助長此類的網路詐騙活動。防範此類勒索軟體攻擊的最好方法是定期備份。您還需要經常更新作業系統、軟體、應用程式以及瀏覽器的更新程式。絕大多數的弱點利用工具將已知的弱點作為攻擊目標，並安裝功能強大的安全軟體，卡巴斯基網路安全軟體有特殊的「系統監控」功能，保護使用者免遭加密病毒的感染，時時保護您的電腦安全。

如果您已經是卡巴斯基產品的用戶，您需要做的是確保卡巴斯基網路安全軟體開啟「系統監控」功能。

趨勢科技 Pc-cillin



有關諾頓產品和 Cryptolocker 威脅的資訊

本文提供有關 Cryptolocker 威脅的詳細資訊。

什麼是 Cryptolocker？

Cryptolocker 是一種會將使用者的檔案加密的惡意軟體。此威脅甚至對企業造成更多的損害，不只是將使用者的檔案加密，連分享或連接網路磁碟機的檔案也會予以加密。

並且有許多 Cryptolocker 的變異體，例如：

- Trojan.Ransomcrypt.I (Cryptowall 和 bitcrypt2)
- Trojan.Cryptodefense
- Trojan.Cryptolocker.E/ Trojan.Cryptolocker.G (CTB-Locker: Curve-Tor-Bitcoin Locker) 也稱為 Critroni

諾頓能夠將我的檔案解密嗎？

被 Cryptolocker 加密的檔案會維持加密狀態。諾頓產品不會將已被這些威脅影響的檔案解密。不過，如果您有使用備份解決方案，可以從之前的備份取代檔案。如果您已經將 Norton Online Backup 設定為備份您的檔案，則可以從中還原您的檔案。

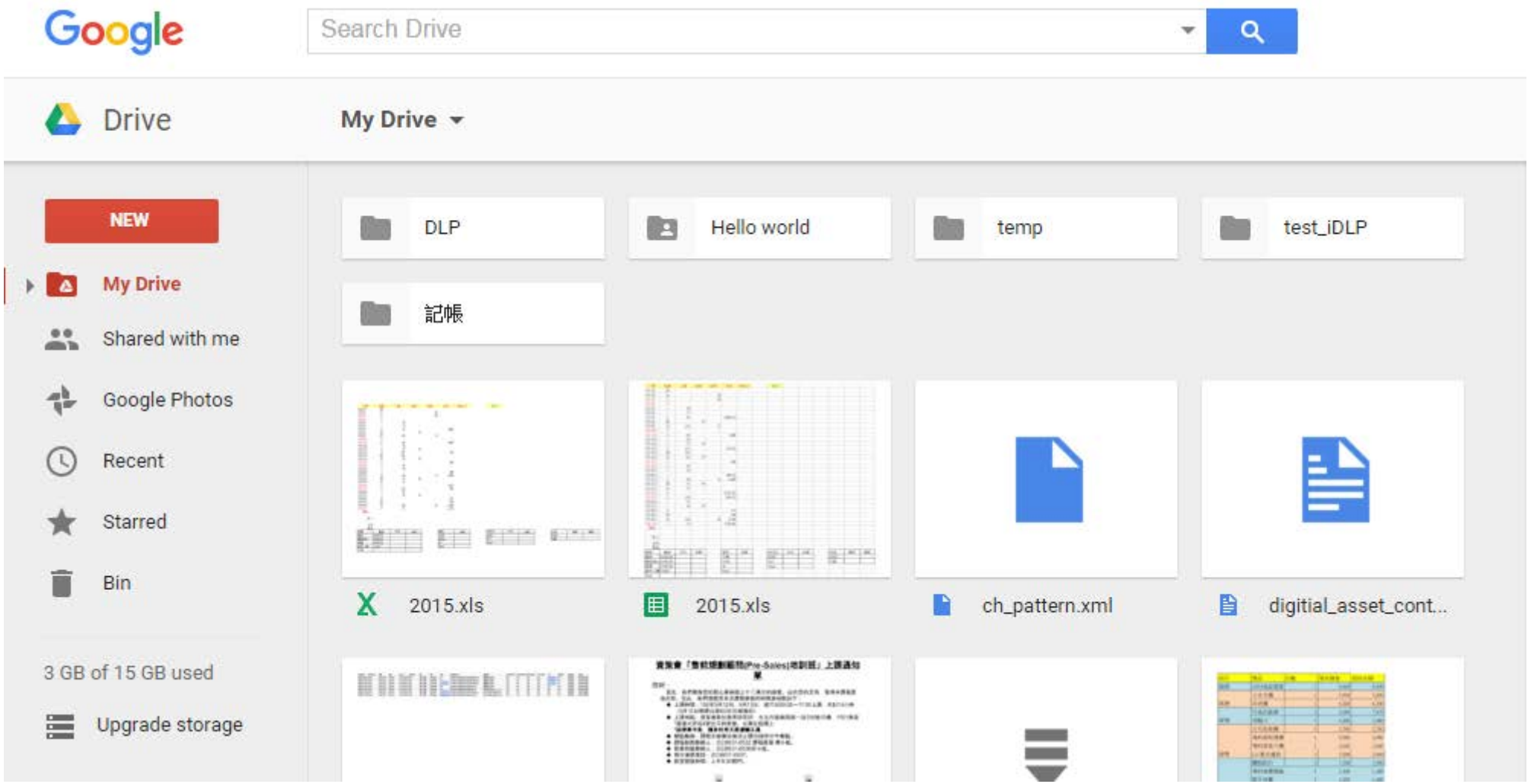
若要得知還原備份檔案的詳細資訊，請參閱從 Norton Online Backup 還原。

保持軟體更新

- 定期執行Windows Update
- 不要亂點來路不明的信件或網站
- 定期更新軟體漏洞
  - Java
  - Adobe Reader
  - Adobe Flash Player
  - 瀏覽器版本(IE、FireFox、Chrome)
- 雖然預防重於治療，但若您的重要檔案都已備份，您至少可以將勒索程式的傷害降至最低。
- 請遵守 3-2-1 備份原則：3 份備份、2 種不同儲存媒體、1 個不同的存放地點。

儲存媒體

Google Drive

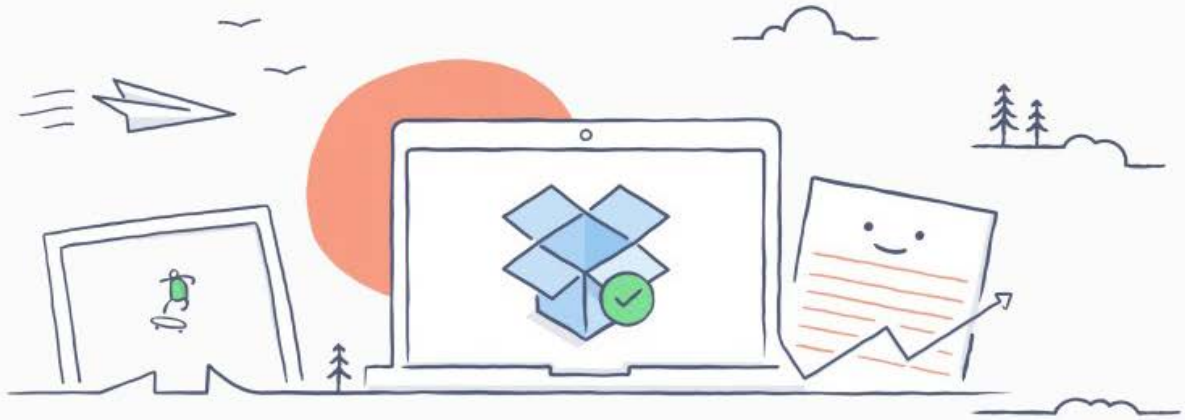


Dropbox

試試 Dropbox Business

Dropbox

下載應用程式・登入



檔案放進來，好事跟著來

Dropbox 會妥善保管您的檔案，讓您隨時保持同步，並輕鬆與他人分享。

姓氏 名字

電子郵件

密碼

我同意 Dropbox 條款。

2T空間夠了吧

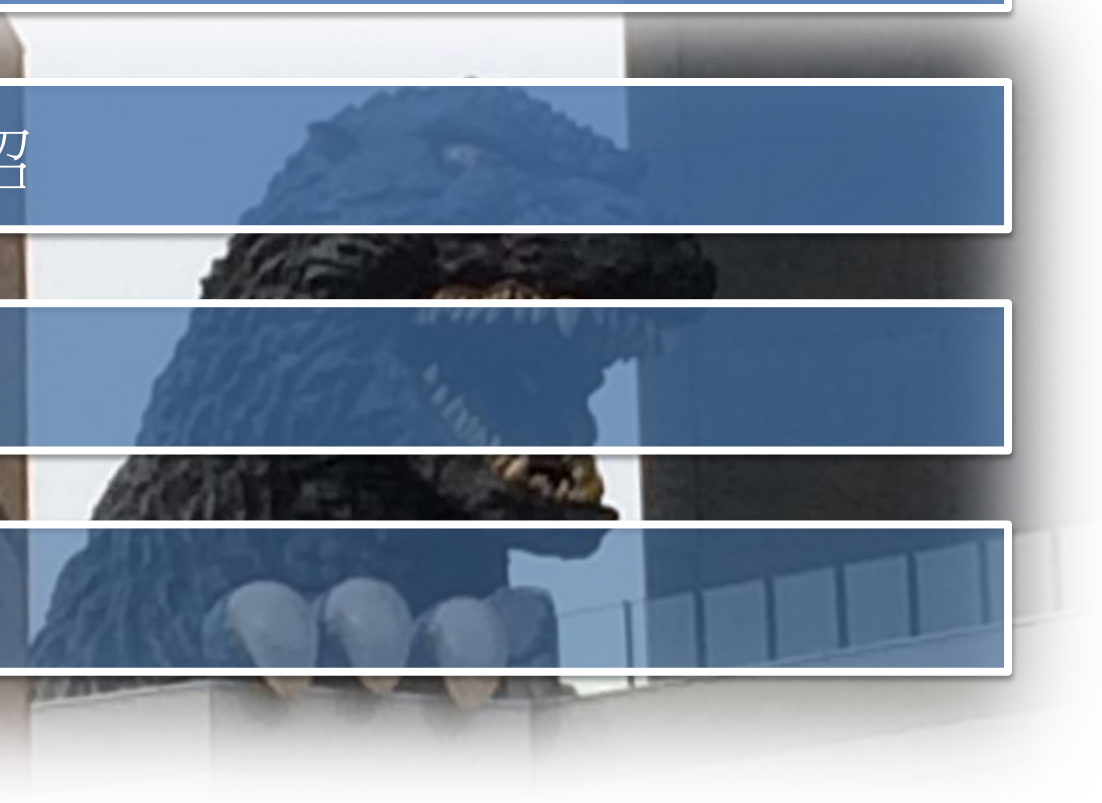
百度云 网盘
严打违规文件和盗版侵权传播 | 百度首页 | 客户
2T大空间
可存200万张照片
2T
PLUS
登录百度帐号
海外手机号
手机/邮箱/用户名
密码
下次自动登录
忘记密码?
登录
可以使用以下方式登录
没有百度帐号？
立即注册百度帐号
Windows
Android
iPhone
iPad
WP
同步盘
扫描二维码下载

企業該如何防護

- 定期執行Windows Update
- 不要亂點來路不明的信件或網站 (定期做社交攻擊演練)
- **增強Web、Mail防禦(文件弱點防護)**
- 建立網路與主機層面的預警行為
- **定時備份重要檔案**
- 定期更新軟體漏洞
  - Java(能不用就不用)
  - Adobe Reader
  - Adobe Flash Player
  - 瀏覽器版本(IE、FireFox、Chrome)

簡報大綱

- 勒索軟體大災問
- 勒贖病毒感染行為與特徵介紹
- 勒贖病毒防禦介紹
- 勒贖病毒案例
- Q & A



SYSTEM INTEGRATION

勒索軟體：恐嚇取財手法十年進化史

自從我們第一次遭遇勒索軟體 Ransomware至今已過了大約十個年頭，這類軟體藉由挾持受害者重要的檔案或系統，然後逼迫受害者支付一筆金額來贖回這些資料 (因而稱為勒索軟體)。為了記錄這個有史以來發展最蓬勃、吸金能力最強大的惡意程式類型邁入十年重大里程碑，讓我們來回顧一下我們所接觸過的重大案例，看看它們這些年來是如何發展與演變。

資料來源：趨勢科技

新聞事件

勒索軟體的起源發展

在 26 年前，勒索軟體這一概念便已出現，首次被記載的勒索軟體是 1989 年的 AIDS Trojan。該威脅透過 5¼ 英寸硬碟中的郵件進行傳播，通過加密電腦上的檔案，要求使用者支付解密費用。 雖然 AIDS Trojan 並非被認為是當今的勒索軟體，但它卻使用了如今常見的伎倆，也就是對使用者使用未授權的軟體所進行的懲罰。

即使 AIDS Trojan 是首次出現的勒索軟體，但實際上，誤導應用軟體(Misleading Applications)和後來出現的偽裝防毒軟體(Fake AV)產品才是造成「數位勒索」趨勢愈演愈烈的罪魁禍首。與勒索軟體相同，誤導應用和偽裝防毒軟體的目的都是向使用者進行金錢勒索。

誤導應用軟體流行於 2005 年，該應用軟體向受害者報告虛假的電腦問題，隨後要求他們支付購買軟體的許可，從而對電腦問題進行修復。基於誤導應用軟體的欺詐手段，Fake AV 在 2008 年和2009 年開始流行，這些欺詐攻擊手法試圖說服使用者其電腦受到惡意軟體的入侵，進而騙取使用者付費購買假的軟體許可。

多年來，公眾對誤導應用軟體和 Fake AV 逐漸有了更深入的瞭解。因此在 2011 年和 2012 年之間，攻擊者轉而使用勒索軟體作為網路犯罪活動的手段。剛開始時，攻擊者通過鎖定勒索軟體(Locker Ransomware)進行

資料來源：http://www.hkitblog.com/?p=30187

加密檔案勒索金錢已經是新一波潮流

駭客入侵醫院主機　挾病例勒索逾1億

美國洛杉磯好萊塢長老教會醫療中心（Hollywood Presbyterian Medical Center）驚傳主機遭到駭客入侵，被勒索9000比特幣（約1.1億元台幣）贖金。翻攝英國廣播公司

根據英國廣播公司報導，駭客是透過「勒索軟體」（ransomware）入侵醫院主機，醫院證實主機被入侵，但不願回應勒索相關細節，但醫院電腦系統已經停擺超過1周，員工需要以紙筆作業，病患的檢測結果也無法以電子檔案寄送，醫院甚至得用電話和傳真與外界聯絡，因為連網路都不通。

洛杉磯警方與聯邦調查局（FBI）已會同資安和電腦數據鑑識專家著手展開調查。院方表示目前分析認為駭客是隨機攻擊，並非針對特定病人竊取病例，對病患影響有限，且院方已安排部分病患轉院，因為醫院檢驗設備、斷層掃描以及藥房等設施也無法正常使用。

根據資安機構統計，近年來醫療機構已經取代金融和零售機構，成為駭客攻擊的主要對象，駭客竊取了大量或特殊名人病歷資料後，會將這些數據在網路黑市中轉賣給犯罪組織獲利。（廖育琳／綜合外電報導）

資料來源: *2016 0217* *http://www.appledaily.com.tw/realtimenews/article/new/20160217/797129/*

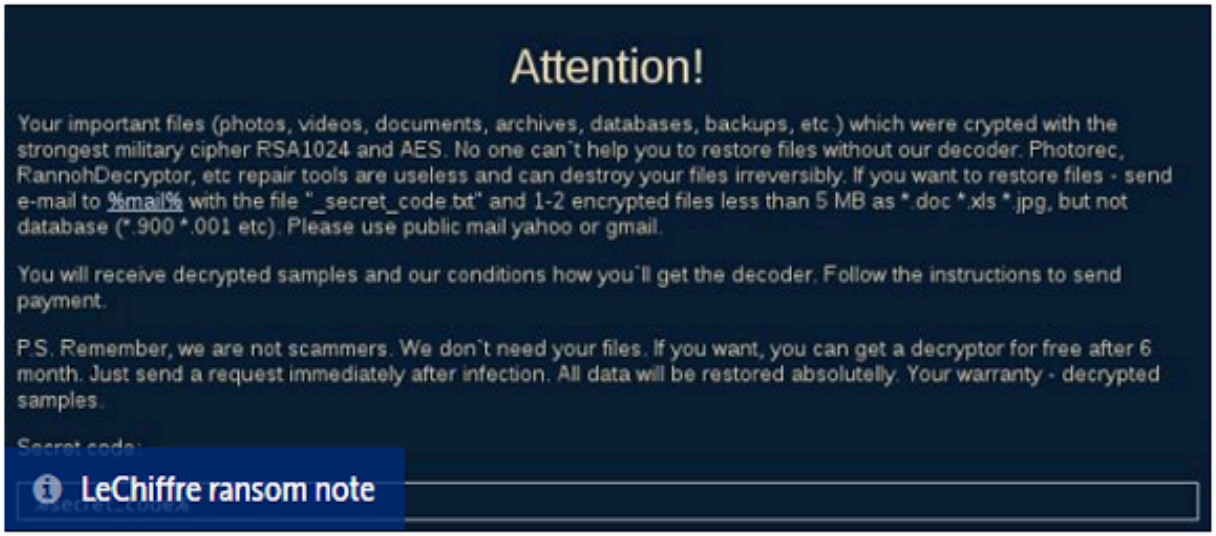
醫院、銀行、高科技為大宗受害者

損失大了！勒索軟體成功侵入三間印度銀行

勒索軟體是去年最可怕的惡意軟體，許多人都遭受到勒索軟體的威脅。不過，個人的資料、照片遭到勒索軟體威脅雖然很痛苦，但是有些時候或許你抱持著「重新再來」的想法，牙一咬也就忍痛犧牲了。但是，如果是一間公司遭到勒索軟體的威脅，那可就不好玩了。更進一步，如果是銀行被勒索軟體控制，那就更恐怖了。

這個月有三間印度的銀行以及一間藥廠公司遭到了LeChiffre系列勒索軟體的威脅，被入侵的電腦遭到加密封鎖，束手無策。

LeChiffre系列勒索軟體與一般的勒索軟體有點不同，它只有透過使用者手動執行，才會啟動加密電腦檔案。因此，駭客的作法是先入侵這些公司的網路，然後在受害者的電腦安裝遠端桌面軟體，當他獲得了電腦的存取權，就再從他的伺服器上下載勒索軟體，然後點選執行，進行勒索加密。



▲LeChiffre跳出的勒索介面以及付款訊息。

鬼月好駭怕!! 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)

POSTED ON 2013 年 08 月 13 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Like 3k Share Tweet G+1 11 Pin it

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。

資料來源：趨勢科技

偽防毒軟體

Facebook Password Reset Confirmation.
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: The Facebook Team
Date: Tuesday, October 27, 2009 4:18 AM
To:
Subject: Facebook Password Reset Confirmation.
Attach: Facebook_Password_7a343.zip (23.8 KB)
Hey a ,
Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.
Thanks,
The Facebook Team
SAMPLE SPAM EMAIL

WinZip - Facebook_Password_7a343.zip
File Actions View Jobs Options Help
New Open Favorites Add Extract Encrypt
Name Type Modified
Facebook_Password_7a343.exe Application 10/27/2009 6:03 AM
Selected 0 files, 0 bytes
Total 1 file, 30KB

Power-Antivirus-2009 2.6
Windows is Secure
Power-Antivirus-2009
Helps protect your PC
System scan
Security
Privacy
Update
Firewall
Settings
Enter activation key
Your security status:
At risk
Activate protection
Scanning for Viruses
INFECTED
Scaning:
Stop
Remove
Path c:\Documents and Settings\All Users\ntuser.pol
Objects scanned: 10719
Recommendations
Scan Results
Scan Infections Found: 2
Power-Antivirus-2009 has found software that might harm your computer or compromise your privacy.
You are highly recommended to remove unknown software
Software
Category
Keylogger.Stawin
Trojan
Remove
Alert level: Medium
Description: Keylogger.Stawin is a keylogging Trojan horse that attempts to steal a user's online banking information.
Spyware.ActivityKey
Spyware
Remove
Alert level: High
Description: When Spyware.ActivityKey is installed, it monitors user activity, logs keystrokes, takes
Remove Threats
Continue unprotected
MALICIOUS PROGRAM

Get rid of dangerous infections, privacy risks and annoying advertising!
1 Year Software License -
69.95 USD One Time Charge
2 Years Software License -
69.95 USD One Time Charge
Lifetime Software License -
89.95 USD One Time Charge
7 Reasons to Buy:
PC MAGAZINE EDITORS' CHOICE
PC MAGAZINE Best of the Year 2005
THE TOP 100 PRODUCTS OF 2006
PCWorld BEST BUY
PC ADVISOR BEST BUY

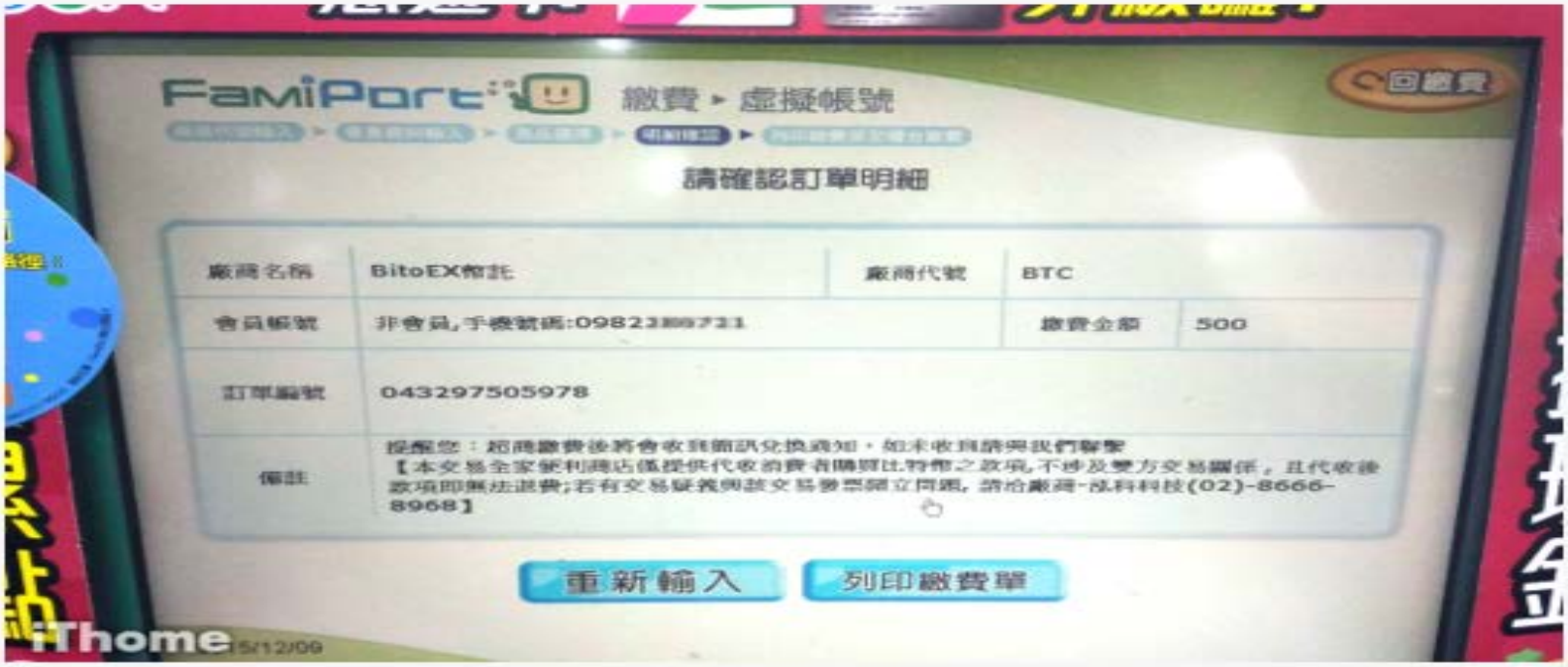
偽防毒軟體

Activation Page
$49,95
THREE YEARS LICENSE
SECURITY ESSENTIALS 2011
Revolutionary Security Essentials 2011 technology provides the fastest protection against malicious threats to your PC. Unlike the competition, the latest and emerging threats are analyzed and blocked in milliseconds. Our product is the most effective and Easy-to-Use protection against virus, online and network threats.
Extra features:
Malware protection.
Virus protection.
Spyware protection.
USB Virus scan.
Active PRO Security.
Billing Info
$49.95 Security Essentials Package 2011 NEW!!
NOW INCLUDING: Specialized Services for home and office!
Three Years License
Add 24h Live Chat (Premium Support). $13.95
Upgrade to Lifetime License + add SE 2011 FireWall. $6.95
First name:
Last name:
Address:
City:
State:
Select state
ZIP Code:
Country:
United States (US)
Phone:
E-mail:
E-mail confirmation:
Credit Card Info
Card number :
(Only Visa or MasterCard)
Expire date:
Exclusive Security Essentials 2011 Firewall technology provides instant protection and the highest detection rates against today's threats. Firewall is a part of a computer system that is designed to block unauthorized access while permitting authorized communications.
Conventional PC user may think that Windows firewall is the best protection. Unfortunately, it gives you a false sense of security, protecting incoming traffic only, excluding outgoing traffic, with your credit card info, social security number, bank accounts, passwords and other confidential information. SE 2011 Firewall installed on our systems give feeling of increased security that your computer and the data are safe and continuously being protected. Get the maximum benefit of using SE 2011 with SE Firewall!
Only for $6.95 more, upgrade Security Essentials 2011 to our most effective protection against virus and online threats.

勒索軟體家族

CoinVault
Bitcryptor
TeslaCrypt
Linux.Encoder.1
CryptoLocker
iThome

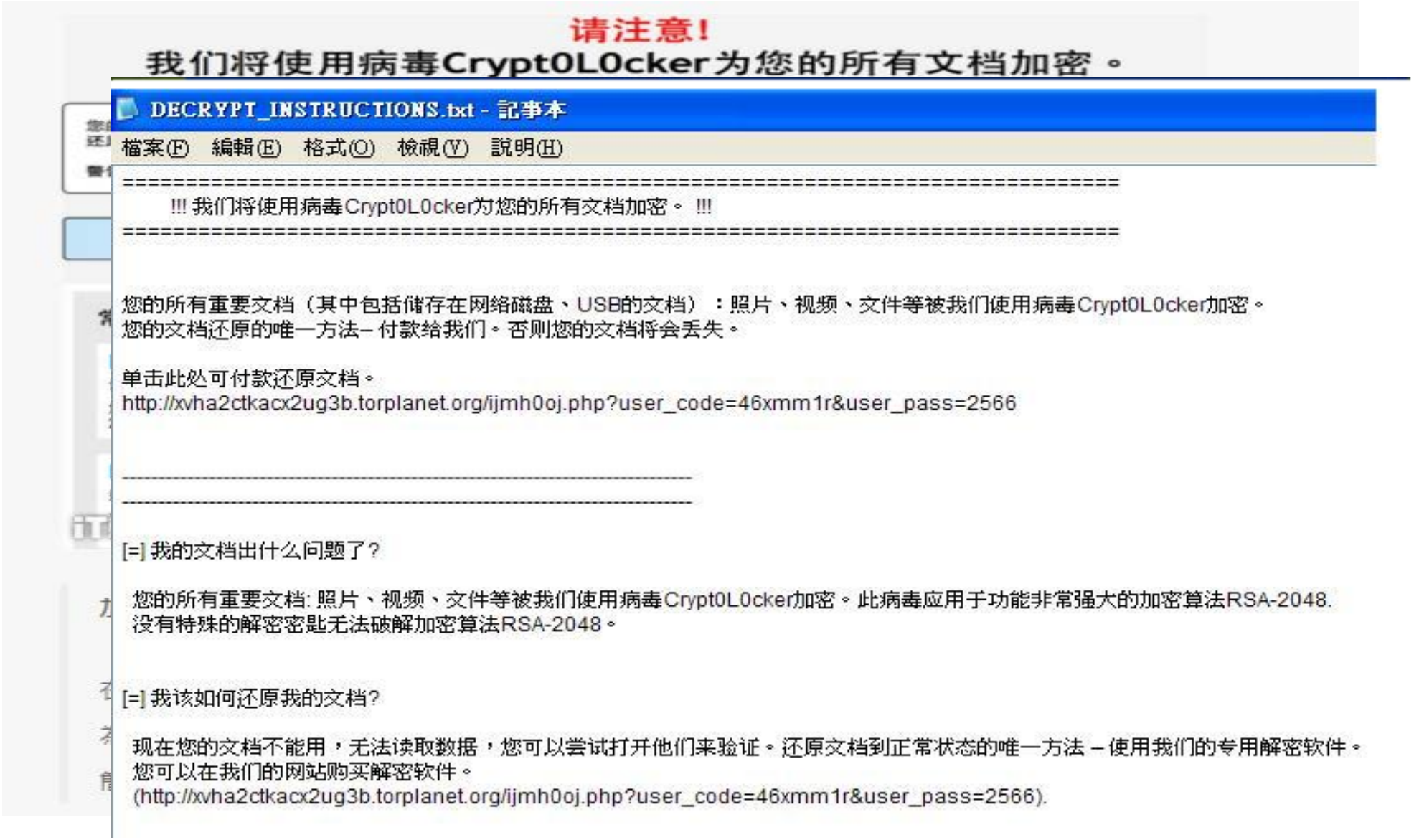
使用比特幣付款



使用比特幣付贖金，是近年勒索軟體的手段

依加密勒索軟體要求買比特幣付贖金，真的是沒有辦法中的辦法。如果你真的決定要那麼做，購買管道已經有，利用遍布全國的全家便利商店FamiPort機臺，選擇繳費、虛擬帳號，輸入BTC或BitoEX代號，之後依循步驟輸入，就能列印繳費單購買，之後只要接收手機簡訊，依步驟線上兌換Bitcoin。

本土客製化



请注意!

我们将使用病毒Crypt0L0cker为您的所有文档加密。

DECRYPT_INSTRUCTIONS.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

==========

!!! 我们将使用病毒Crypt0L0cker为您的所有文档加密。 !!!

==========

您的所有重要文档（其中包括储存在网络磁盘、USB的文档）：照片、视频、文件等被我们使用病毒Crypt0L0cker加密。
您的文档还原的唯一方法– 付款给我们。否则您的文档将会丢失。

单击此处可付款还原文档。
http://xvha2ctkacx2ug3b.torplanet.org/ijmh0oj.php?user_code=46xmm1r&user_pass=2566

[=] 我的文档出什么问题了？

您的所有重要文档: 照片、视频、文件等被我们使用病毒Crypt0L0cker加密。此病毒应用于功能非常强大的加密算法RSA-2048.
没有特殊的解密密匙无法破解加密算法RSA-2048。

[=] 我该如何还原我的文档?

现在您的文档不能用，无法读取数据，您可以尝试打开他们来验证。还原文档到正常状态的唯一方法 – 使用我们的专用解密软件。
您可以在我们的网站购买解密软件。
(http://xvha2ctkacx2ug3b.torplanet.org/ijmh0oj.php?user_code=46xmm1r&user_pass=2566).

加盟事業

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 搜尋

新聞

勒索
勒索

Cryptolocke
或是移至他

文/ 陳曉莉 |

根據CSO報導，一個名為Fakben的駭客團隊最近推出Cryptolocker Service勒索軟體服務，客戶只要支付50美元就能下載Cryptolocker執行檔，開始勒索事業。該軟體還能設定勒索金額，以及用來收錢的比特幣帳戶。只是Fakben將索取勒索金額的10%作為服務費。

Cryptolocker是在2013年9月問世的勒索軟體，它利用郵件附加檔案及殭屍網路進行散布，以將受害者電腦中的檔案加密，但遞送Cryptolocker的殭屍網路Gameover ZeuS已於2014年5月遭多國警方聯手破獲，警方還取得解密私鑰的資料庫，當時估計Cryptolocker的攻擊者已成功取得300萬美元的贖金。

不過，Fakben團隊向CSO Online透露，他們雖然使用與Cryptolocker一樣的名稱，但程式碼是截然不同的。這代表該軟體有別於已可被多數防毒軟體攔截的Cryptolocker。

這並不是市場上第一次出現「勒索即服務」的商業模式，今年初也有一個名為Tox服務標榜可提供客製化的勒索軟體，並索取勒索金額的30%以作為服務費。

勒索軟體感染趨勢統計

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社
比例的中小企業遭受攻擊，如何應用現有的資源有效防範，是相當大的挑戰
文/ 周峻佑 | 2015-12-19 發表
讚 2.1 萬 按讚加入iThome粉絲團
讚 分享 383
G+1 40
2015年下半加密勒索軟體
威脅再起
單位（千個）
50
40
30
20
10
0
48
36
20
28
21
23
16
31
34
35
39
44
2014年 11月
12月
2015年 1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
根據資安公司的調查，加密勒索軟體近期有明顯成長的趨勢，像是日前防毒廠商賽門鐵克，發表10月份的網路安全威脅報告（ISTR），數據顯示，全球電腦感染加密勒贖軟體的情況，從2014年11月的高峰之後趨緩，但從2015年6月份開始趨勢轉變，最近9、10月份更是屢創今年單月份新高，威脅擊高趨勢值得用戶注意，資料來源：趨勢科技，iThome整理製圖，2015年12月

Mac 也難逃

首例！Mac 電腦遭勒索軟體攻擊

資安軟體製造商 Palo Alto Networks 的威脅情報中心總監歐爾森（Ryan Olson）周日透過電話採訪向路透社表示，這款名為「KeRanger」的惡意軟體於 4 日出現，是首款攻擊蘋果 Mac 電腦的勒索軟體（ransomware）。

勒索軟體過去主要攻擊微軟（Microsoft）的 Windows 作業系統用戶。資安專家估計，這類型網路犯罪的受害者合計每年支付數億美元贖金。

Palo Alto Networks 指出，攻擊 Mac 電腦用戶的駭客，主要透過知名檔案分享軟體 Transmission 進行攻擊。用戶若下載於 4 日釋出的 Transmission 2.90 版，就會受到勒索軟體感染。

Palo Alto Networks 表示，惡意軟體 KeRanger 的潛伏期約 3 天，換言之，若 Mac 用戶 4 日遭受 KeRanger 感染，他們的電腦今天就會連上駭客伺服器，電腦上的檔案也會被加密無法使用。一旦加密程序完成，KeRanger 會要求支付 1 元比特幣當作取回檔案權限的贖金，相當於 400 美元（約新台幣 1.3 萬元）。

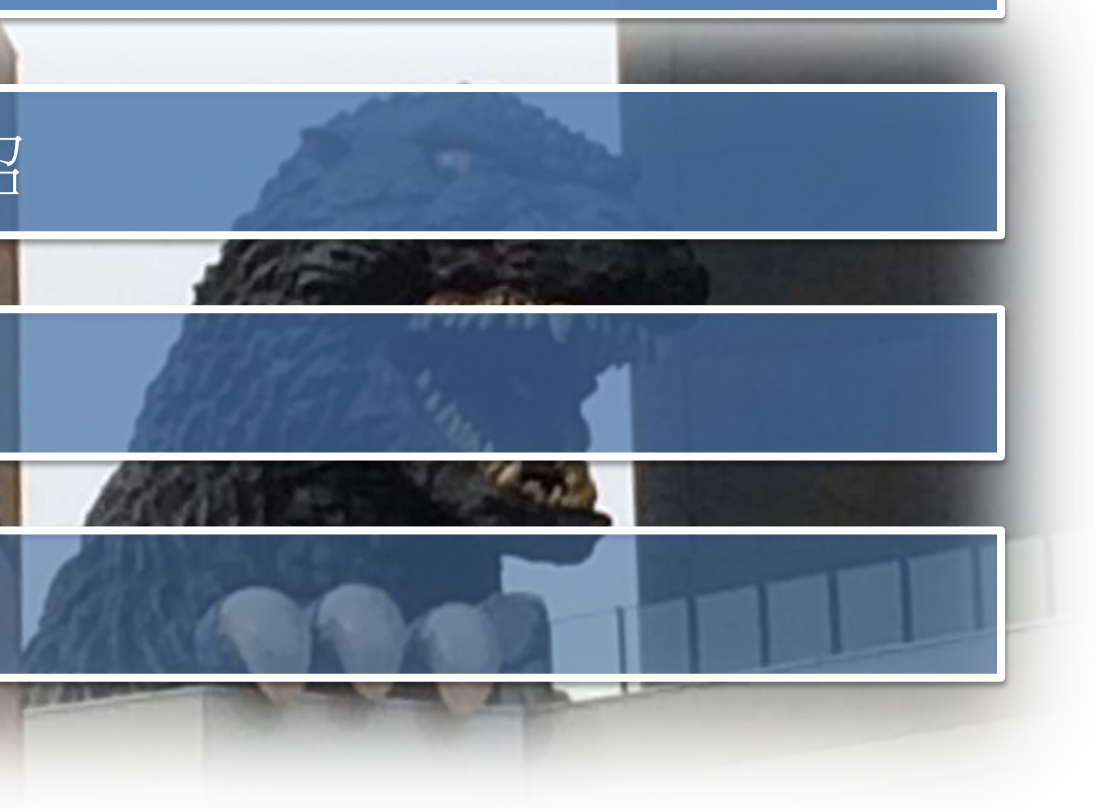
Transmission 網站建議，用戶若有被感染疑慮，應立刻升級到 2.92 新版軟體。蘋果表示，公司已於上周末撤銷 Mac 電腦安裝該款惡意軟體的數位憑證，防止更多電腦遭感染，但拒絕提供進一步細節。

最後.....備份才是王道

備份！備份！備份！
至少一定要用外接硬碟備份！

簡報大綱

- 勒索軟體大災問
- 勒贖病毒感染行為與特徵介紹
- 勒贖病毒防禦介紹
- 勒贖病毒案例
- Q & A



Thank You

謝謝

麟瑞科技
RING LINE CORPORATION

邁向卓越 穩健踏實
www.ringline.com.tw