勒索軟體（**Ransomware**）

今日犯罪有逐漸朝網路發展的趨勢，隨著資訊量越來越多，人們不但開始慢慢習慣新的數位時代，更對資訊的依賴也更加強烈，舊式詐騙集團也開始改弦易轍。低風險、高報酬的誘因，讓詐騙集團紛紛投入網路犯罪這塊新的領域。

□ 何謂勒索軟體 Ransomware？

勒索軟體 Ransomware 是一種特殊的惡意軟體，駭客利用木馬程式或釣魚郵件等將表面上不會對系統造成迫害的軟體殖入電腦中，等到用戶不經意觸發執行該軟體，就會與伺服器連線並啟動該軟體的功能，讓你失去對自己系統或資料的控制，駭客團體再經由此軟體發佈訊息，此訊息大概的意思皆為如果要讓電腦恢復原狀必須經由付費的方式來達成。基本上，你的系統或資料成為了人質，讓你被迫去支付贖金，這也就是它被稱為「勒索軟體」的原因。

□ 勒索軟體的來源

最早的勒索軟體出現於 2005 年，發生於俄羅斯境內，其後開始全球傳播，發展出許多不同的版本。某些類型的勒索軟體會偽稱為當地的警察機構，將這些勒索付費稱之為「贖金」，再轉變以「罰款」的形式出現，讓使用者不得不馬上支付，更甚者還有透過本土語音訊息傳播勒索公告。

□ 勒索軟體的傳播模式

1. **假冒知名網站商發佈釣魚郵件進行傳播（Chrome、Facebook、PayPal 等）**
2. **透過惡意網址進行木馬及不明軟體安裝**
3. **惡意執行檔圖示變更為 PDF 圖示，使用者誤以為是 PDF 檔點擊後感染**

□ 執行該軟體所造成的危害

該惡意軟體會嘗試連接被勒索者所控制的伺服器，成功連接後伺服器就會**產生一組 2048 位元的 RSA 加密金鑰配對**，並且送出公開金鑰到被感染的電腦，同時也會有效將整個硬碟與其相連結的網路硬碟中的檔案，利用公開金鑰進行加密，並將檔案加密的記錄存入一個登錄碼，這個過程中，會將特定副檔名的資料進行加密。

□ 駭客源頭追捕困難

CryptoLocker 伺服器可能是一個本地或其它的代理伺服器，會頻繁地在不同國家間進行重新定位，造成追蹤源頭的困難度。

□ 勒索程度

- 被害 PC 索價 11,900 台幣或 300 美元，或是 2 比特幣。
- 72 小時未付款，私人金鑰將會在伺服器端摧毀，並且無法打開這些被加密的檔案。

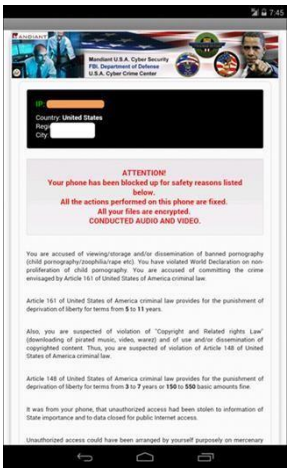
- 超過 72 小時，付款價格將會增長到 10 比特幣。（約 3,250 美金）
- 一旦被駭導致檔案經加密演算法被鎖，目前無可行的解法。
- 因加密共享文件而會占用公司頻寬，區域會變得很緩慢。

□ 勒索軟體的近況

2013 年有一個特別麻煩的勒索軟體稱為**「Cryptolocker」，它會加密重要檔案，只有當你支付贖金後才提供解密方法，Cryptolocker 變種使用無法破解的加密演算法，**所以使用者只能選擇乖乖付錢（隨然可能不會真的解密檔案）或失去他們的資料。

➢ 勒索軟體甚至還從一般電腦發展到 **Android** 系統上

一個過去鎖定電腦散播勒索軟體 Ransomware 的惡意集團 Reveton，現在將要求贖金的目標改為 Android 手機，通常是會瀏覽色情網站的訪客。

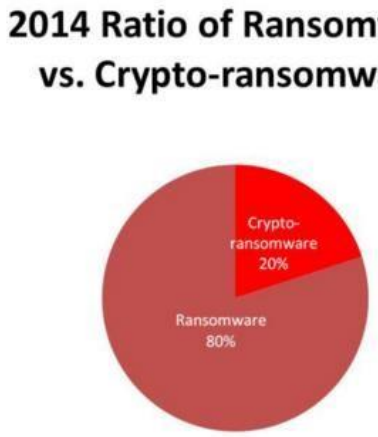


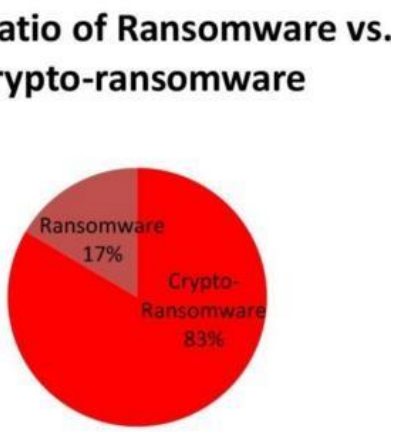
Reveton 是純粹的勒索軟體，它具有系統層級的存取能力，能導致受害者的手機無法運作，被害者為了讓手機恢復原狀，必須透過歹徒指定的付款機制支付 300 美元贖金，才能取回手機使用權。

一旦行動版 Reveton 感染了手機，它會出現來自看似各地執法單位的假警告。比如在美國會出現「Mandiant U.S.A Cyber Security / FBI Department of Defense / U.S.A. Cyber Crime Center」。他們會針對用戶的地理位置查找手機的 IP，並利用一些當地執法單位的招牌來顯示客製化的頁面讓某些人的手機突然變磚，直到可以在網路上取得他們所要的贖款。

被害者為了讓手機恢復原狀，必須「透過難以追查的付款機制」（如 Paysafecard 或 Ukash）來支付 300 美元，並不像一般電腦上的 CryptoLocker 勒索軟體 Ransomware 會加密手機上的所有資料，行動版 Reveton 是純粹的勒索軟體，它在所有介面和使用者介面中加入一中介程式，也因為惡意軟體具有系統層級的存取能力，所以使用者無法做任何事情。

從 2013 年起，我們所偵測到的傳統勒索軟體與加密勒索軟體的比例，已從過去的 80/20 演變至今日的 20/80,甚至還從一般電腦發展到 Android 系統上。起初加密勒索軟體主要鎖定歐美國家，到了 2015 年，勒索軟體開始出現簡中介面，臺灣爆發災情，受害者包含企業和個人用戶。





前一陣子有位台北市某公司會計人員，誤點免費中獎 iPhone 6S 的釣魚郵件，導致伺服器上的資料被勒索軟體 CryptoLocker 加密，結果當事人與主管調離現職。根據 2015 年金毒獎票選，「勒索軟體肆虐台灣」公認為今年最驚世駭俗的資安攻擊事件；另一項

2015 年度資安關鍵字票選活動,第一名也由 CryptoLocker(加密勒索軟體)奪魁，得票數占 42.11%。

不僅企業是勒索軟體 Ransomware(勒索病毒/綁架病毒)攻擊目標，個人用戶受害者也不計其數，它會鎖住你的電腦或加密你的檔案直到你付錢為止，通常會有一個最後繳交贖款期限。現在它變得比以往任何時候都更加凶狠，在 2014 年，趨勢科技所偵測的 48,000 個樣本中有 15,000 個是「加密勒索軟體」，這代表自 CryptoLocker 以來增加了 27%，

CryptoLocker 是一年前所出現此類惡意軟體的始祖。

資料來源：趨勢科技，iThome 整理製圖，2015 年 12 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，威脅攀高趨勢值得用戶注意。

□ 如何防範勒索軟體？

「您的帳戶欠款已過期」一打開"欠款明細"附檔，即刻中招！「你的檔案已被加密，支付 600 美金索取解鎖金鑰，96 小時後贖金加倍，倒數計時開始！」一旦看到勒索訊息往往為時已晚，勒索軟體胃口愈來愈大，如果你採信 FBI 花錢消災的建議，得有即使付錢也不能保證檔案會重新回到身邊的心理準備，更慘的是食髓知味的駭客，知道攻擊目標會乖乖就範，有不少案例顯示駭客會發動另一波更高金額的攻擊，再度挾持檔案當肉票。

勒索軟體不會很快地消失，它已經有效地擴散到其他平台，像是 Android 系統。如何保護自己防範勒索軟體 Ransomware？**你可以採取以下四個步驟和『三不三要』口訣預防：**

1. **不要打開未確認的郵件或點入它們內嵌的連結，那可能會開始安裝勒索軟體。**
2. **採用 3-2-1 規則來備份你的重要檔案：在兩種不同媒介上建立三個備份，其中一個備份要放在不同的地方。**
3. **定期更新軟體、程式和應用程式以確保其維持在最新狀態，可以防範新的漏洞。**
4. **最後建議使用提供勒索防護功能的軟體來保護你的電腦。**

□ 勒索軟體的未來發展：開始朝行動勒索軟體發展

除了社交工程（social engineering）技巧、雙重加密以及不斷演化的惡意程式之外，歹徒更不斷提升其運作的隱密性。他們將提供給受害者聯繫並支付贖金的網站架設在 Tor (洋蔥路由器) 網路上，將其惡意程式暗藏在數百或數千個已遭入侵的網站上，將每一個被加密檔案的系統備份刪除。除此之外，TorrentLocker 有時還會使用「CryptoLocker」這個名字，造成使用者在分析流量記錄時的混淆。未來，隨著商務逐漸朝行動化發展，行動勒索軟體的攻擊案例將日益增加。在地下市場上，勒索軟體的買賣已成為一大商機，我們必須認知一點，網路犯罪集團和一些政府背後支持的駭客，都已開始將最新的
CryptoWall 和 TorrentLocker 版本納入他們廣大的行動當中。趨勢科技網路安全長 Tom Kellermann 指出：「勒索軟體 Ransomware 之所以蓬勃發展，正因為網路犯罪集團看到了它的發展潛力和容易取得的特性。」

資安廠商趨勢科技網路安全長 *Tom Kellermann* 指出：「勒索軟體之所以蓬勃發展，正因為網路犯罪集團看到了它的發展潛力和容易取得的特性。但最令人擔憂的是它已開始朝行動勒索軟體發展。」

恐嚇的伎倆加上進階惡意程式，讓加密勒索軟體犯罪集團能不斷從受害者身上獲利。尤其，我們在歐洲、中東、非洲、紐澳、北美等地區看到的這些迅速準確的攻擊行動，證明了我們有必要採取一些新的資料保護方法。沒有一種解決方案可以提供完整的防護。我們必須找出歹徒行動的方式、地點、時機及動機。很重要的一點是，企業必須與資安廠商密切合作，借助他們豐富的專業知識來對抗加密勒索軟體的威脅。兩者的結合才能有效蒐集、分析、回應今日最迫切的威脅。歹徒決不會放棄任何可大賺一票的機會，因此這類攻擊對企業造成的成本只會越來越高。要解決這些問題，我們必須防禦技術與人員雙管齊下，建立一套更聰明防禦機制以防範歹徒挾持資訊，確實保護我們的資訊安全。

資料來源

[1] GDATA－惡意勒索軟體（Ransomware）－ http://www.gdata.tw/index.php?option=com_content&view=article&id=619:ransomware&catid=91:20160106&Itemid=228

[2] 何謂勒索軟體 (Ransomware) ?(含歷年勒索軟體與贖金)－ http://blog.trendmicro.com.tw/?p=11161

[3] 認識 Cryptolocker 等勒索軟體/病毒(綁架病毒) ,該如何預防？(內有資料圖表)－ http://blog.trendmicro.com.tw/?p=12412

[4] “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－ http://blog.trendmicro.com.tw/?p=8614

[5] 不給錢就讓手機變磚塊!勒索集團威脅瀏覽色情網站 Android 手機用戶－ http://blog.trendmicro.com.tw/?p=8211

[6] 加密勒索軟體捲土重來，大舉攻擊小型企業與個人用戶－ http://www.ithome.com.tw/tech/101364

[7] 中了勒索軟體/病毒怎麼辦？只能付款了事嗎? 牢記四步驟和"三不三要"口訣－ http://pccillin.pixnet.net/blog/category/1130752

[8] 勒索軟體令人意想不到的經營手法!－ http://blog.trendmicro.com.tw/?p=14200