技術文章

加密勒索軟體捲土重來，大舉攻擊小型企業與個人用戶

在2013年CryptoLocker出現之後，加密勒索軟體成為駭客有效的獲利模式，因此不只是大型企業，也有極高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

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。資料來源：趨勢科技，iThome整理製圖，2015年12月

最近在網路上一個靠北工程師的貼文，在資訊人員之間廣為流傳：一間位於臺北市的公司，因為會計人員點選釣魚郵件裡，免費中獎iPhone 6S的消息，導致ERP伺服器上的資料被CryptoLocker加密，影響業務報價、倉儲盤點，連各部門的差勤打卡系統也無法使用，如此誇張的描述，不禁讓人想問，公司要倒了嗎？

最後的結果，該名會計人員與主管調離現職，伺服器資料全部重新建置。這個故事之所以引起資訊人員的注意，就是這樣的案例，很有可能就在你我身邊發生，而且像CryptoLocker這種加密勒索軟體，它會將硬碟上的資料加密，受害的使用者只有放棄資料，或是在期限內支付贖金解鎖兩種選擇，若沒有駭客手上的解密金鑰，基本上無法解鎖。

但是，照著駭客的指示，支付贖金，未必就能順利取回檔案。日前趨勢科技在萬聖節

但是一無者駭客的指示，支付贖金，未必就能順利取回檔案。日前趨勢科技在臺灣即時針對消費大眾調查，發現接近4成的民眾，最害怕的就是勒索軟體，遠超過信用卡遭盜刷、手機被定位追蹤、網路攝影機偷窺等金錢損失與隱私受到侵害的比例，因此，這類軟體已經造成人心惶惶，電腦若是感染此類病毒，幾乎只能任由駭客擺布。

不同於一般的病毒，加密勒索軟體針對的是使用者電腦裡的檔案，因此清除這類軟體未必困難，甚至若想要支付贖金為檔案解鎖，還可能必須依賴它。

這類手法真正可怕之處，在於檔案加密之後，就完全無法使用，而這些檔案包含使用者經年累月存放在電腦裡的文件、照片、影片等等，一般而言，中毒之後，通常只要換到另一臺電腦，或者是將電腦重新安裝作業系統，大致上就能繼續工作。但檔案遭到加密之後，無論那一臺電腦都無法讀取，使用者面臨支付贖金，與檔案損失這種進退兩難的情況。

以往我們害怕電腦病毒，多半就是這些程式會導致電腦無法正常運作，有的則是暗地中收集個人隱私，神不知鬼不覺。不過，現在駭客的想法已經改變，癱瘓用戶的電腦對於他們不見得有意義，但挾持使用者的電腦檔案，這門生意顯然有利可圖。

像CryptoLocker這樣的加密勒索軟體，自2013年在臺灣造成災情之後，近期似乎又有大幅興起的趨勢。這兩個月以來，許多電視臺再度爭相報導，呼籲使用者自保，包含重要的資料應備份到外接硬碟、定時更新防毒軟體，以及收到不明信件別亂點連結與附件等措施。而根據賽門鐵克的2015年10月份資安報告，加密勒索軟體在今年的下半年攻擊陸續增加，甚至10月份已經幾乎追上去年最顛峰的狀態。

依據趨勢科技的報告，今年的6至7月間，加密勒索軟體攻擊手法，有接近7成的比例是針對中小企業，顯示這些企業需要正視這個情況。

另一方面，自我們2014年底報導過加密勒贖軟體更加本地化，出現日文版勒索介面之後，現在也有以簡體中文，說明如何支付贖金的方法，畢竟臺灣不少公司兩岸三通，同時在中國大陸與臺灣設立辦公室或是工廠，中文化也顯示這類攻擊手法越來越普及，並且更針對當地，已不密臺灣的企業單位專外。

及，並且更針對當地，已不容臺灣的企業置身事外。

超過三分之二的中小企業遭受CryptoWall攻擊

中小企業用戶受害最嚴重，不得不防。就趨勢科技2015年6到7月份的觀察，勒索軟體攻擊對象比例中，中小企業（SMB）佔了相當高的比率，有67.23%，等於超過三分之二。他們並表示，多數打開CryptoWall相關電子郵件內惡意連結的使用者，都屬於中小企業用戶。

資料來源：趨勢科技，iThome整理製圖，2015年12月

CryptoWall家族是2015年數量最多的勒索軟體

根據資安公司的調查統計，隨著加密勒索軟體的成熟發展，現在已有不少勒索軟體家族趁勢興起。以今年第3季來看，CryptoWall所屬的CRYPWALL家族，發動最頻繁，相關的垃圾郵件數量最多。（註：每個資安公司對於勒索軟體家族，名稱上可能會略有不同）

資料來源：趨勢科技，iThome整理製圖，2015年12月

TorrentLocker主要攻擊對象

也是中小企業與一般人

趨勢科技在2015年6到8月份的觀察中，大多數TorrentLocker受害者，會收到一封看似正常網址的電子帳單郵件，點了連結之後，導致感染加密勒索軟體，其中，中小企業與一般用戶受害的比例均接近一半。

資料來源：趨勢科技，iThome整理製圖，2015年12月

感染徒徑主要來自釣魚郵件，但也出現透過軟體漏洞植入的手法

以前述的故事和統計數據而言，反映出不少在企業中，可能會面臨到的資訊安全問題：包括使用者的資安意識嚴重不足、管制政策與資安防護有待加強等面向。

俗話說得好，知已知彼，百戰百勝。在面對這樣的情勢，受威脅的標的物，是可以備份的文件檔案，換言之，若在有效的備份前提之下，使用者可能就不需要傷腦筋檔案救不回來，甚至無須理會駭客漫天開價的贖款金額。但事實上，在企業中，光是個人端點的備份，就難以要求像防毒一樣落實。

另一方面，如果能知道感染這類病毒的來源，自然也能多加以留意，減少重要文件受到加密的風險。趨勢科技資深技術顧問簡勝財表示，加密勒索軟體主要的攻擊管道，還是在於釣魚電子郵件、網頁惡意程式與惡意廣告，以及透過論壇文章瀏覽等管道。

簡勝財說，目前而言，加密勒索軟體最大宗的攻擊方式，還是透過電子郵件的釣魚手法，因此光是使用者避免點選這類連結，或是附件檔案，就能大幅減少中毒的機率。不過，這種電子郵件可能會冒用朋友、同事、政府機關的身分寄送，而附件也可能偽裝圖示，假裝是Word文件等常見檔案，實際上卻是有問題的可執行檔，但要防範或是查證，並沒有非常困難。

在NEC負責Cyber Security戰略本部的經理田正明，則進一步表示，現在在日本，公司的人資部會經常接收到假藉應徵者求職的釣魚郵件，而一般個人，則是可能會看到透過電子訃文郵件包裝的攻擊手法，這兩種電子郵件，更難透過用戶自行辨識郵件的真

實性，與附件的安全，雖然以目前臺灣似乎還沒有看到的類似手法，但類似這種情況，極有可能是未來會發生在你我身邊的攻擊方式，也將會更加難以防範。因此，在NEC內部，除了新人教育訓練即包含有關資安項目，甚至會不定期以釣魚郵件，測試並提升使用者的資安意識。

不過，透過使用者點選釣魚郵件導致中毒，已經不是感染的唯一途徑。賽門鐵克首席提術顧問張士龍表示，有客戶向他反應，只是開啟瀏覽器上網，沒有下載任何檔案，之後卻發現電腦的文件檔案已經全數加密，張士龍檢查發現，這起事件中，駭客很可能就是透過瀏覽器的漏洞，在使用者的電腦中植入惡意程式，因此這個用戶在不知不覺的情況下，受到這種攻擊，因此他認為未安裝最新的Windows修補程式，更新瀏覽器程式與Flash Player，留給駭客可利用的漏洞，也是相當有可能的感染途徑。

事實上，駭客對於加密勒索軟體的手法也推陳出新，不只是透過釣魚電子郵件，等待使用者點選上鈎，不少也開始直接針對瀏覽器、Windows作業系統、Adobe Flash Player等軟體的漏洞，採取在網頁上植入惡意程式的手法，因此，只要瀏覽這樣的網頁，就可能大開這類軟體後門，駭客直接取得系統權限，將電腦檔案加密。

尤其最近一、兩年來，經常被發現這些軟體的零時差漏洞，軟體公司不見得會即時推出修正程式，而推送給使用者時，用戶也不一定會安裝，這種情況也很容易造成有心人士利用的途徑。

甚至，有些駭客也以廣告主的身份，透過購買網路廣告，以內含惡意程式的廣告，而進行這類網頁木馬的散布，可說是神不知鬼不覺，難以預防。對於不會瀏覽某些有安全疑慮網站的使用者而言，也可能受到這種手法的攻擊。

此外，對於從非官方來源下載檔案，也有機會下載到夾帶這類的惡意程式的軟體。因此對於檔案的來源，仍然最好是來自於軟體廠商的官方網站。

加密勒索軟體已有中文提示訊息介面

在早期，大部分加密勒索軟體事件都是國外案例，從去年開始，亞洲中文地區也成為針對性攻擊的目標，像是CryptL0cker這款加密勒索軟體的提示介面，就是顯示簡體中文。而位處臺灣的我們，也需多加留意這種攻擊的入侵。

勒索軟體十年進化：病毒變種，採用比特幣付款，難以追查來源

在加密過程中，大多數的加密勒索軟體，會修改這些所要綁架文件檔案的副檔名，表示這些檔案已經加密，有些還會在資料夾下加入純文字或HTML格式的讀我（Read Me）檔案，提醒使用者，想要解開，就要支付贖金才行。

不過，手法的日新月益，有些新的變種軟體更是改用亂碼更名，讓使用者無從找起，自己有那些檔案遭受加密。

從勒索軟體演進歷史來看，最早可追溯至2006年的TROJ_CRYPZIP.A，這是一個可以將指定類型的檔案，以密碼保護的壓縮檔打包之後，刪除原始檔案的病毒。而這個檔案還會留下一個具有勒索文字的記事本檔案，告訴使用者可以300美元的代價，取得壓縮檔的密碼。

演進至2011年，開始出現鎖住螢幕要求付贖金的程式，例如鎖定俄羅斯用戶的TROJ_RANSOM.QOWA，它一改挾持檔案的作法，直接將使用者的桌上型電腦鎖住，並在螢幕上顯示一個要求支付12美元贖金的畫面。受害者必須撥打一個付費電話號碼，同意支付費用，才能取回系統的主控權。

隨著時間演進，2012年這種鎖定螢幕的勒贖軟體，更直接假冒FBI或是當地的執法機關，藉此恐嚇使用者，誤以為自己使用非法軟體，遭到警方盯上，心生恐懼而付款。

到了2013年，就是現在最可怕的加密勒索軟體始祖CryptoLocker出現，但與2006年的做法明顯不同，它同時採用兩道加密的方法，第一道是以AES金鑰將檔案加密，第二道則是透過RSA演算法加密前述的金鑰，這是一種加密與解密金鑰不同的演算法，因此受害者無法直接進行反向解鎖，必須透過駭客手上的金鑰才能取回檔案，於是使用者只有兩個選擇，選擇付贖金，或是捨棄檔案，當時也有不少臺灣的企業受害，是這一波的災情開始。

甚至這樣的攻擊，也會影響到網路儲存硬碟NAS，2014年8月，一種名為SynoLocker的變種加密勒索軟體，針對群暉科技（Synology）NAS舊版DSM作業漏洞攻擊，對於採用該廠牌NAS的用戶產生影響。

由於這種模式，已經成為駭客有效的獲利管道，今年資安公司更發現多種變種程式，例如專門綁架線上遊戲的Teslacrypt、首個透過Tor匿名網路進行勒索的CTB-Locker，鎖定日本使用者的TorLocker，以及鎖定俄國企業的Kryptovor等等，而付贖款的方式，也由一般的轉帳匯款，改為要求使用數位貨幣比特幣（Bitcoin）支付，藉此躲避追查。

最近，更出現可離線執行的新型變種軟體，即使切斷網路，也無法阻擋其加密行為。

加密勒索軟體威脅大事紀

2006年　開始有加密勒索攻擊事件

TROJ_CRYPZIP.A會要求使用者支付300美元，才能取得壓縮檔的密碼。

2011年　加密勒索處於實驗成長階段

在贖金的付款方式上，已經能接受行動支付機制。

2013年9月　Cryptolocker現身

當時便有臺灣企業受害，是這一波加密勒索災情的開始。

2013年9月　攻擊手法本土化

TorrentLocker會利用當地國家在意的議題，誘使使用者點擊垃圾郵件，
後續並有變種TorLocker

後續並有變種TorLocker

2014年8月 鎖定NAS為勒索對象

SynoLocker鎖定群暉NAS舊版DSM漏洞進行攻擊，建議用戶更新至已修補的最新DSM版本。

2015年1月 史上威脅最大，第3代CryptoWall

據CTA安全聯盟估計，CryptoWall為駭客集團帶來獲利3.25億美元。最近並演進到4.0版本。

2015年2月 鎖定知名遊戲綁架

Teslacrypt會對遊戲寶物或點數等相關檔案，進行AES加密。

2015年11月 勒索門檻降低

有駭客團隊推Cryptolocker SaaS服務，讓客戶能快速開始勒索事業。

2015年11月 Linux也受害

Linux.Encoder.1將利用電子商務網站常用的Magento CMS漏洞，將主機資料加密。

2015年11月 出現不需C&C的勒索軟體

可離線執行、不需連到C&C伺服器的加密勒索新型態。

資料來源：趨勢科技、賽門鐵克，iThome整理，2015年12月

勒索軟體受害途徑大解析

入侵手法1 社交工程郵件（釣魚郵件寄送附件或有害連結）

利用釣魚信郵寄，欺騙使用者開啟附件，或是點選附件中的有害連結，這種利用人性弱點的方式，若使用者不夠警覺，就有可能受害，若結合更多偽裝手法，像是檔名或圖示的偽裝，甚至偽裝電子郵件與內容，使之看似正常通知信，更令人難以防範。

階段1 使用者收到夾帶惡意附件或有害連結的釣魚信。

階段2 使用者若沒有警覺，下載附件並執行，或是點選有害連結，便啟動了加密勒索軟體。

階段3 加密勒索軟體連至中繼站取得金鑰開始加密，完成後跳出勒索贖金的畫面。

入侵手法2 軟體漏洞造成（網頁掛馬、惡意廣告程式）

利用像是Windows、Java、Flash或瀏覽器的漏洞，讓使用者在瀏覽網站時受到感染，若是用戶電腦沒有時常更新這些軟體，或是安裝防毒軟體，就有很大的機率受到感染。甚至，也有駭客以廣告主身份，向合法廣告供應商購買流量，以惡意廣告形式傳播。

階段1 使用者瀏覽了遭植入一段惡意連結的網站，且網頁外觀看起來都很正常。

階段2 加密勒索軟體會透過軟體漏洞，背景自動執行，使用者在不知情的狀況下受害。

階段3 加密勒索軟體連至中繼站取得金鑰開始加密，完成後跳出勒索贖金的畫面。

入侵手法3 網路芳鄰

一臺PC主機若遭受加密勒索病毒攻擊，除了該臺電腦本身受害，萬一同時還有外接硬碟、USB隨身碟，或具有網路磁碟機、雲端硬碟、檔案伺服器的存取權限，這些與受感染電腦相連的檔案也會遭到惡意加密。另外，有些病毒也能透過網路芳鄰方式，感染其他連線主機。

階段1 使用者具有網路資料夾的存取權限，但意外感染加密勒索軟體而不自知。

階段2 除了本機內的資料，網路資料夾中的檔案也同時被勒索軟體加密。

入侵手法4 網站論壇非法軟體

若使用者從論壇下載非法軟體，其中也有可能被植入加密勒索攻擊程式，讓用戶因貪小便宜的心態，主動受感染。

階段1 當用戶從網站論壇下載非法工具程式並執行。

階段2 一旦啟動軟體，等於同時啟動加密勒索軟體。

入侵手法5 USB感染

USB隨身碟也是常見的病毒擴散方式，只要電腦插上受病毒感染的USB碟，通常會搭配autorun.inf檔案，讓電腦主機也會跟著中毒。

階段1 當隨身碟插入中毒端電腦，即將病毒寫入，也將autorun.inf檔案寫入，企圖使該隨身碟有傳染力。

階段2 當隨身碟再次插入其他電腦時，使用者只要從「我的電腦」點兩下USB磁碟，透過autorun.inf檔的運作，觸發執行病毒。

資料來源：趨勢科技、賽門鐵克，iThome整理，2015年12月