面對(加密)勒索軟體
什麼是該做，什麼是不該做

您應事前做好準備保護重要檔案，不要向勒索軟體屈服

目　錄

前 言

多數人覺得“綁架勒索”只會發生在好萊塢電影及黑幫老大身上，但其實網路犯罪者正在使用勒索程式對企業進行要脅，攻擊各種大型及小型目標。根據賽門鐵克最新一期的2015年網路安全威脅研究報告第20期指出(ISTR 20)，截至2014年底，全世界約有**17億**個惡意程式。單單2014一整年，就增加了約**3.17億**個惡意程式，也就是**一天約增加1,000,000(一百萬)**個惡意程式。而在2014這一年，平均每個月有729,167個勒索程式攻擊。勒索程式攻擊在2014年增加了**113%**，從2013年的410萬上升到880萬。值得注意的是檔案加密勒索程式的成長（賽門鐵克稱為“加密勒索程式”），從2013年的8,274增加到2014年的373,342個。**在一年的時間內，加密勒索程式成長了45倍**。2013年，加密勒索程式只佔所有勒索程式的0.2%(500分之1)，同時也非常不普遍。但是到了2014年底，就成長到佔所有勒索程式的4%（25分之1）。

加密勒索程式的危害程度

- 不只攻擊受害電腦內的重要文件和檔案，也會搜尋受害電腦連結的網路芳鄰、網路磁碟機、檔案伺服器等，攻擊公司內網所有共享的檔案。一旦中毒，這個勒索軟體不只是會影響單一電腦，更會感染公司內部網路的所有檔案。
- 發出勒索訊息後，受害電腦無法上網，也無法開啟遭加密的文件。
- 加密後，使用者無法自行復原。
- 即使成功付贖金取得金鑰，也有少數檔案無法使用。
- 惡意程式加密內網共享文件時，會占用頻寬，導致內網速度超慢，受害電腦效能也會大減。

加密勒索程式的運作方式

- 加密勒索程式會使用非對稱加密(asymmetric encryption)技術，把電腦檔案及內聯網絡的檔案加密。檔案類別包括Office、PDF…等文件、圖片、相片、影片、繪圖編輯檔、數據庫檔案及電子憑證檔案等等。
- 加密後，惡意程式會把加密密鑰回傳到指令及控制伺服器(C&C server)，並在受感染的電腦留下勒索訊息，要求用戶支付指定金額的比等幣(BitCoin)，以換取解密密鑰，否則唯一的解密密鑰將被刪除。
- 由於加密勒索軟件使用高強度加密算法，因此，在沒有解密密鑰的情況下，被加密的檔案無法回復。這會導致公司的業務運作受到嚴重影響。

加密勒索程式的感染途徑

- 加密勒索程式的感染途徑，與一般的惡意程式如：病毒／蠕蟲／間諜程式…如出一轍。除了釣魚電郵、網頁式攻擊(如順道下載、水坑式攻擊…)，亦會透過其他途徑來進行傳播，包括P2P程式分享檔案，更新假冒Flash Player，及安裝假冒的多媒體播放程式等。
- 加密勒索軟體很多都是透過釣魚電郵感染電腦，釣魚電郵會載有壓縮檔案附件(zip檔案)，內裡包含一個偽造PDF文件的執行檔(exe檔案)。當用戶打開這個執行檔案，電腦便會受到感染。
- 最近，新變種的加密勒索程式碼會插入DOC文件檔內，透過釣魚電郵發送給受害者。若用戶打開DOC文件檔及允許巨集(macro)程式執行，電腦便會受到感染。

站在人性角度，勒索程式是最骯髒的一種攻擊方式。罪犯使用惡意軟體來加密受害者硬碟－家庭相簿、作業、音樂及未完成的小說－要求付錢才會釋放檔案。最嚴重的竟然是，只有保持分開的檔案備份，然後再離線重新備份，才有辦法防衛。

目前已有許多勒索程式變種，並且所有作業系統都可能遭殃。忠告就是：**千萬別付錢給罪犯**--許多企業及個人只是想要找回檔案，所以他們付了錢，讓這些罪犯有利可圖。雖然有不少方法可以對付這些不法之徒，然而最重要的還是防範未然，別讓不法之徒有機可乘。

去年Sony Pictures爆發嚴重資安事故，據悉在事發前公司高層就曾收到勒索信，揚言不付錢就會發動攻擊。其實類似的勒索事件非常多，很多中小企都不幸中招。但資訊安全專家就警告別向勒索軟體屈服，因為付了錢也不一定能贖回重要檔案，因此**日常做好資安防護和備份就很重要**。

勒索軟體如CyptoLocker、CrptoWall、CryptoDefense及CTB-Locker在企業間十分猖獗，這些勒索軟體目的都是十分簡單：以偷去的資料作為要脅，向受害人勒索金錢。我們必須明白甚麼是勒索軟體，它們對企業做成甚麼影響及危機。最重要是面對這些勒索軟體，有甚麼是該做，有甚麼是不該做，避免成為受害者。

壹、我的資料／檔案被勒索軟體加密，該怎麼辦？

- **重點：不要屈服，不要付款！**
  付款等於鼓勵，即使你付款，你可保證你能完整地重新取得原先的檔案嗎？切記這些不法之徒是在要脅你。如果大家還記得電影《贖金風暴》裡，兒子被綁架，爸爸不屈服，寧願把贖金當成懸賞獎金不付款，最後才能把匪徒繩之以法。
- 立即切斷受駭PC的網路，避免災情擴大。加密勒索程式不只攻擊受害電腦內的重要文件和檔案，也會搜尋受害電腦連結的網路芳鄰、網路磁碟機、檔案伺服器等，攻擊公司內網所有共享的文件。
- 更新防毒軟體，清查區域網路內的其他電腦，並採取自保措施。
- 搶救還沒被加密的檔案。不要再利用該台電腦開機，可將該硬碟卸載後外掛於其它非重要電腦進行搶救檔案及病毒掃描等修復作業。

■ 若有備份，開始復原檔案。

■ 謹慎評估受害災情，決定是否付贖金取得解密金鑰。**不太建議，因為沒有資料顯示支付贖金一定能取回解密密鑰並成功回復檔案。另外，有可能因為加密勒索程式的指令及控制伺服器(C&C Server)已遭到破獲，即使支付贖金，也未能取回解密密鑰。**

■ **從好的備份回復任何受影響的檔案，這是最快而安全的方法。**

■ 如果系統沒有備份，我們建議用戶暫時不要重裝系統，以免加密檔案記錄資料遺失，導致後續的修復變得更困難。

■ 若使用雲端備份，請確認雲端服務提供版本紀錄(version history)功能。即使受影響的檔案已同步到雲端，這功能可以回復檔案到之前版本。

■ 平常及事發後可經由查看企業版的端點防護系統的中央主控台(如SEP的SEPM)、郵件安全閘道(如SMG)以及網頁安全閘道(如SWG)的日誌，有助益於及早發現異常的安全狀態，對於預防及事後修復與安全政策改善有很大的幫助。

貳、我可以拿回我的檔案，而不用向不法之徒付款或者從備份裡修復嗎？

很可惜這世上沒有這樣的事。不法之徒通常都把一些檔案勒索並且隱藏，留下原裝檔案但會使用「磁碟區陰影複製服務」（VSS），或者把副本以加密形式留在本機裡。這很值很詳細地調查變種資料，看看有甚麼解決方法，但通常都是徒勞無功，因為不法之徒會比你早一步洞悉先機，預先想像你會有何對策。

參、我可以從加密檔案裡以Brute-Force(暴力攻擊法) 打開我的加密檔案嗎？

不能。現時的威脅以RSA-2048數位加密，Brute-Force對他們只是小兒科。

肆、我該怎樣防範勒索軟體？

■ 安裝、妥善配置(設定)以及強制執行端點防護解決方案(SEP)

» 端點是防禦任何威脅的最後一道防線，應該採用一個多層次的安全解決方案。這個解決方案應該具備不只是基於檔案威脅的防護（傳統防毒軟體），而且還應該包括下載防護、瀏覽器防護、啟發式技術、防火牆和社群來源檔案的信譽評分系統。

»Symantec Endpoint Protection 12.1（SEP 12.1）的用戶可以套用在安裝 SEP 12.1 時自動產生的「高安全性」病毒和間諜防護政策提供防止受到勒索軟體的威脅。通常會直接編輯預設的政策，具體詳細的政策設置訊息，可以查看此文件 http://www.symantec.com/docs/TECH173752

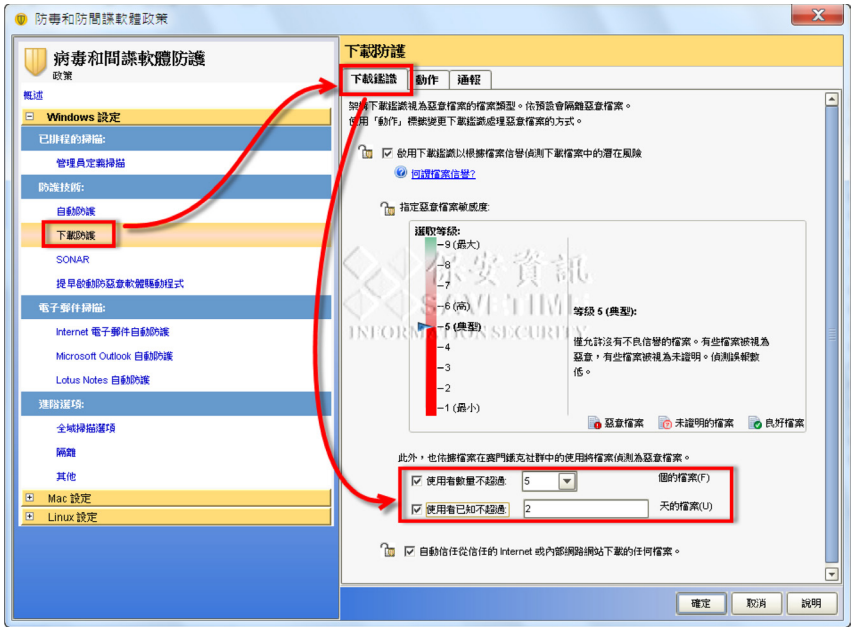
» 要強化防護新勒索軟體的變種，可以編輯「高安全性」政策並修改該政策中的下載防護功能，啟用尚未被賽門鐵克用戶社群證明是好的檔案。需要改變的選項位於「下載防護」-「下載鑑識」-「此外，也依據檔案在賽門鐵克社群中的使用將檔案偵測為惡意檔案」。啟用兩個選項「使用者數量不超過 x 個的檔案」

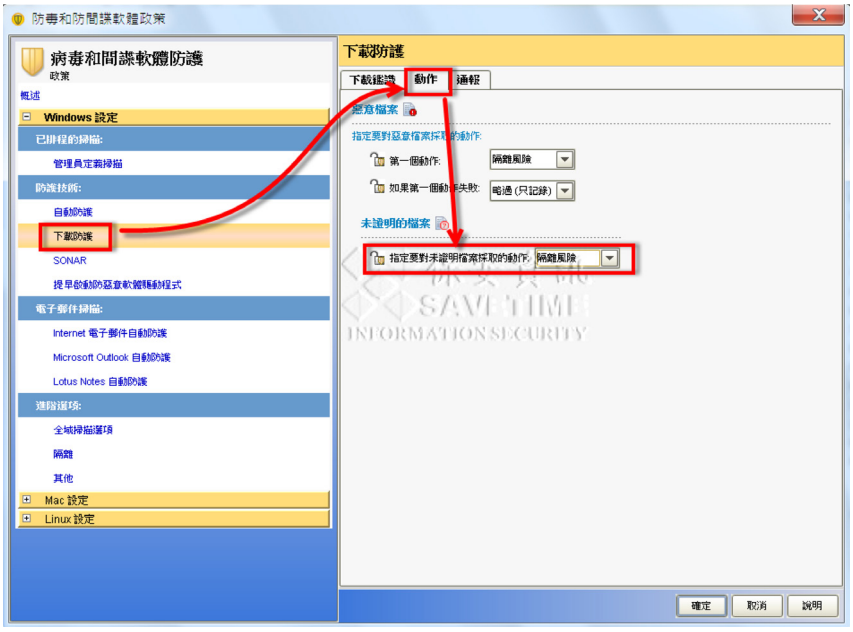
和「使用者已知不超過 x 天的檔案」，並使用 5 和 2 的預設值分別強制對 SEP 12.1 的用戶端做處理，已回報給賽門鐵克但回報數量少於 5 個用戶或已回報但還不到 2 天的任何檔案被視為未經驗證的檔案。

»**SEP 的應用程式控制政策可以限制檔案的存取，所以針對勒索病毒我們可以攔截系統去產生加密檔案進而達到阻止勒索病毒的運作此政策禁止系統建立以下附檔名的檔案（可以自行增加）：（保安資訊有提供圖文並茂的 SOP 文件下載）**

.crypted/.encrypted/*.ezz/*.ecc/*.exx/*.VAULT/*.bitcrypt/*.bitcrypt2/*.atxczxb/*.ctbl/*.ctb2

» 在「動作」頁籤下，「未證明的檔案」和「指定要對未證明的檔案採取的動作」應設置為「隔離風險」。





» 使用所有端點防護解決方案的通則，是應該參考廠商所提供的如何設定在上網行為的即時掃描選項。讓它盡可能以「高安全性」防毒和防間諜政策且任何流行的檔案由他們的使用者為基礎作決定。

» 更符合您企業內部不同架構與安全等級需求的 SEP 政策制定，歡迎與保安資訊聯繫。保安資訊累積十餘年的惡意程式防護的專業經驗，對多面向的端點安全的建議，能提供務實可靠的經驗分享。

■ 教育使用者

這些威脅其實是來自釣魚式攻擊，如來自不知名電郵附帶不知名連結及附件檔案，結果就在無知情況下跌入陷阱。教育員工，對這些電郵提高警覺。

1.不要開啟來路不明的郵件、不要開啟可疑郵件的附件檔案及其附加連結，特別是壓縮檔(.zip、.7z)或執行檔(.exe)及短網址網頁。

2.立即更新防毒軟體。並立即執行防毒軟體掃描。

3.立即備份檔案，並確保備份檔與電腦隔離（或將備份檔改成唯讀狀態）。

4.落實每天備份和掃毒。

5.個案探討：在台灣以中小企業居多，**業務人員**及**研發人員**深受企業主所倚賴。所以在資安的政策上，往往提供較大的自由與方便性。而**方便性與安全性天生就有互斥性**。業務人員看到**訂單、合約、交貨、付款、折扣**等關鍵字的電郵時，幾乎不加思索就會打開。甚至發生過從來沒有接洽過也不認識的假冒買主發了內含加密勒索程式的偽裝訂單附件檔，第一封電郵還大辣辣地說明為確保附件在傳遞中的安全性與保密性，所以該附件檔有加密，密碼請參考隨後的電郵通知，然後第二封電郵就提供開啟該附件的密碼，結果一輸入該密碼，整個硬碟資料就被加密了。而**研發人員**，也會收到一些專用開發/設計/繪圖軟體所產出的檔案，就會不加思索地開啟。而**惡意程式發送者，就常常在附件檔案的名稱上動手腳**，例如：ABCDEFG-**PDF**.exe、12345678-**DWG**.exe、12345678-**psd**.exe。CorelDRAW（附檔名為**cdr**）、Illustrator（附檔名為**ai**、**eps**）、Freehand（附檔名為**fth**、**eps**）、Photoshop（附檔名為**tiff**、**jpg**、**eps**、**PSD**）、Indesign（附檔名為indd、pdf）等等。大家看到檔名有上述幾個常用的檔案類型，卻往往疏忽了**其實它是一份有危險性的執行檔**。其它像是**人資**（對求職網來信，電郵主旨是應徵或履歷等關鍵字，較無戒心）、**會計**（對稅務單位的來信，電郵主旨是發票／退稅／憑證等關鍵字，較無戒心）。普遍而言，特定領域的專業人士，對其平時互動頻繁的往來對象，常會因信任之故而毫無戒心，最容易遭受假冒的惡意程式的社交工程危害。

■ 在電郵伺服器上或郵件閘道器使用多層次防護技術

任何外來電郵 (Inbound e-mails) 應該要受到掃描以偵測威脅，在電郵裡阻擋任何可能有威脅的附件或惡意連結。可參考https://www.savetime.com.tw/new_symantec/SMG.asp

■ 導入網頁安全閘道器

網頁安全閘道，可保護組織抵禦 Web 2.0 的威脅 (包含惡意 URL、間諜程式、病毒及

其他類型的惡意軟體)，並提供使用網路與應用程式的控管。對網頁型的惡意程式攻擊，提供非常重要的防護。可參考https://www.savetime.com.tw/new_symantec/swg.asp

■ 為任何作業系統 / 應用程式 / 瀏覽器及其外掛對已知的漏洞進行即時的修補程式更新

任何網站上可下載的東西都有機會散播惡意程式。平日多檢查軟體有否欠缺修補程式，可補充此漏洞。

■ 安裝及配置主機型入侵防護系統

1.IDS 或 IPS 系統可以偵測和阻止通訊企圖，即惡意程式用來建立加密資料所需的公鑰和私鑰。

2.Symantec Endpoint Protection (SEP) 用戶端的 IPS 系統預設會攔截這類型的通訊流量。

■ 在你的終端用戶攔截可以被執行的惡意程式

1.SEP使用者可以利用賽門鐵克提供的應用程式和裝置控制政策範例，防止檔案在根或使用者的%APPDATA%子目錄被執行，以防止被下載的威脅被執行。該政策會攔截檔案的執行嘗試，包括從壓縮格式被解壓出來的執行檔、攔截Auto-Run、腳本檔案和防止從可移動式磁碟執行檔案。

2.企業可考慮推行軟體限制政策，透過GPO可以建立軟體限制政策並設定以達到類似任務，最重要是不要讓員工隨便下載無相關的軟體。

■ 限制使用者存取網路磁碟機

目前勒索威脅能夠瀏覽並加密終端使用者可以存取的任何映射磁碟 (網路磁碟) 的資料。限制分享磁碟或檔案系統底層映射磁碟的使用者權限將可以限制這些勒索軟體有加密的能力。

■ 部署及維持完善的備份解決方案

最快的方法還是把重要檔案進行備份，當出現問題時還有補救的機會。不只伺服主機需要備份，就是一般的工作站的重要檔案也要備份。即便無法佈署專業的備份解決方案，將重要的檔案複製到可攜式的儲存媒體(光碟片，隨身碟，隨身硬碟…)，然後從系統將該媒體卸載，那麼當受到這些 (加密) 勒索軟體類型的威脅影響時，這些備份將為您提供一個保障的資料。

以上資訊旨在幫助您避免被網路罪犯所利用，並防止和預防這些類型的攻擊。這絕不是一個足以保護你的簡潔計劃，但肯定會降低你的風險。下一頁的“**數位勒索：勒索程式的簡短歷史**”，值得參考。

賽門鐵克在端點、郵件安全閘道與網頁安全閘道的第一名解決方案，對於防護包含加密勒索程式以及進階持續性攻擊--APT防護，效益卓越，值得導入建置：

- **端點安全 (企業防毒) 第一品牌**
  https://www.savetime.com.tw/new_symantec/sep.asp
- **郵件安全閘道第一品牌**
  https://www.savetime.com.tw/new_symantec/SMG.asp
- **網頁安全閘道第一品牌**
  https://www.savetime.com.tw/new_symantec/swg.asp

數位勒索：勒索程式的簡短歷史

作者／Peter Coogan

摘自 ISTR 20(賽門鐵克網路威脅研究報告第20期--2014 一整年)

2014年，**加密勒索程式**是新聞常客，在持續進行的勒索程式長篇故事中，已經成為最新且最致命的趨勢。加密勒索程式不同於標準的勒索程式，不再只是簡單鎖住裝置，而會更進一步加密淪陷裝置中的檔案，在很多案例中，會讓受害者再也無法挽回資料。無論是加密勒索程式及勒索程式，都是要讓企業付出贖金才能解除感染。

這類型的惡意軟體其實已經出現十幾年了，但最近這幾年快速成長，結果就是讓網路罪犯由**假防毒軟體(FakeAV)**的製作，轉向有利可圖的**勒索程式**，然後再進階到**加密勒索程式**，惡意軟體的作者們總是不會停下腳步。我們可以清楚看到威脅版圖已經出現了新的領域，數位勒索正在流行。

假防毒軟體（又稱為FakeAV或流氓安全軟體），會以詐欺手段誤導裝置，或是誤導用戶付款來移除惡意軟體。這類軟體已經存在很長一段時間－流行的高峰在2009年，賽門鐵克當時觀察到，共有4,300萬流氓安全軟體安裝在250種不同的程式中，而人們會以30到100美元來購買這些軟體。

勒索程式是一種惡意軟體，會鎖住受感染電腦並拒絕存取。惡意軟體接下來會顯示勒索訊息，運用社交工程方式命令支付贖金才會移除限制。在2012年，賽門鐵克報告指出勒索程式威脅升高，想要移除限制，在歐洲會勒索50到100歐元贖金，美國則是200美元。

現在，在惡名昭彰的Trojan.Cryptolocker出現於2013年後，惡意軟體作者更將他們的注意力轉移到加密勒索程式威脅，讓**整合創新技術、平台及逃避戰術的加密勒索程式**出現在2014年，新舊手法都在從受害者身上撈錢。

2014年最賺錢的加密勒索程式是Trojan.Cryptodefense(又稱Cryptowall)。這項威脅出現於2014年2月底，最初被作為Cryptodefense推出。它運用了Tor及比特幣技術來進行匿名，同時還有強大的RSA-2048資料加密，以及迫使受害者付錢的壓力戰術，一開始的勒索金額是500歐元及美元。

如果付款沒有準時的話，很快就會增加到1,000歐元及美元。根據分析，由於該惡意軟體的作者疏於執行加密功能，把金鑰留給了人質讓他們可以自行逃脫，也就是說把私人加密金鑰留在系統裡了。在這項資訊公開後，這個問題馬上就被惡意軟體作者修補，同時改名稱為Cryptowall。之後，Cryptowall就持續被改良，擁有特權漏洞評估、反分析檢查功能，甚至還使用了I2P（Invisible Internet Project）來進行通訊匿名。Crytowall的已知獲利至少是每個月34,000美元，研究人員估算在那**六個月期間，它至少賺取了100萬美元**。

Windows個人電腦是勒索程式作者最有利可圖的領域，案例持續增加中。但是在2014年，攻擊者更開始針對新的平台進行數位勒索，我們看到了Reveton推出了Android勒索程式，就是已知的Android.Lockdroid.G(又稱為Koler)。透過使用TDS（Traffic Distribution System），Reveton會執行三管齊下的勒索程式攻擊，根據特定的情況需求執行，例如瀏覽器會被用來檢閱由罪犯所控制的網站，流量會被引導來配合勒索程式。

勒索程式開始獨立於平台，Android用戶會被引導下載Android. Lockdroid.G。Internet Explorer用戶會被引導到Angler Exploit套件，傳遞Trojan.Ransom-lock.G.有效載荷，以即將Windows、Linux或Mac所使用的瀏覽器引導到Browlock。其他的勒索軟體類型，會試圖鎖住電腦，簡單運用他們的網頁瀏覽器來敲詐金錢。

在2014年6月，第一個Android檔案加密勒索程式Android.Simplocker被發現。在俄國發動首波攻擊，並在2014年7月前升級到英文版本(Android.Simplocker.B)，利用FBI社交工程主題。在2014年10月被觀察到出現Android.Lockdroid.E(又稱Porndroid)，再一次使用假的FBI社交工程主題。這項威脅同時也使用裝置照相機來拍照，之後即顯示勒索要求。Android.Lockdroid之後引發了多項新的變種，包含病蟲類型功能，可以透過受感染裝置的簡訊自我複製寄發給聯絡人清單，同時還搭配社交工程技巧。

勒索程式作者開始回顧過去的行動裝置，試圖找出可以勒索金錢的目標，他們了解到**網路儲存設備（NAS），所以開始鎖定這項可以儲存大量檔案的裝置**。

Trojan.Synolocker(又稱Synolocker)，運用先前未知的Synology DiskStation管理軟體，**鎖定Synology NAS裝置**，以取得裝置存取權並加密所有檔案要求贖金。這些裝置雖然已經都更新過以預防未來攻擊，但這項案例顯示出**勒索程式作者正在持續尋找新的攻擊領域**。

為什麼勒索程式變動如此之快？因為勒索軟體對網路罪犯來說是有利可圖的事業，贖金的要求範圍從100到500美元不等。在2014年，我們看到**比特幣付款**方式，成為許多最新勒索程式的選擇。比特幣的**強烈匿名性**，讓網路罪犯可以輕鬆隱藏不法所得並進行**洗錢**。

當我們觀察到新的勒索程式家族蓬勃發展時，賽門鐵克同時也看到整體成長的路徑。**自2013年以來，勒索程式攻擊增加了113%，加密勒索程式擴增了45倍以上**。有利可圖激勵了攻擊與新勒索程式數量的增加，不像贖金型詐騙可能很快就會掉出攻擊版圖，勒索程式未來更應該會持續成長。

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承 (Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有IT Team的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的IT Team，經由常態性的教育訓練、精簡的快速手冊以及標準SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保安資訊：

  保安資訊有限公司

  http://www.savetime.com.tw

  0800-381500、0936-285588