ISTR

特別報告：

2016 年勒索軟體與企業

Symantec

目錄

圖表和表格

報告摘要

勒索軟體已迅速成為企業與消費者所面對到最危險的網路威脅，全球損失現在可能已達數億美元。

在過去一年中，勒索軟體的成熟度和威脅能力已進入新的境界。主要的勒索軟體組織能將他們的惡意程式散佈到數以百萬計的電腦上。受勒索軟體攻擊的使用者發現，他們的寶貴資料已被牢不可破的強大加密方式鎖住。

因為勒索軟體運作模式的完善，攻擊者無不充滿淘金心態，想從中牟利的攻擊者也越來越多。感染數字呈現攀升走勢，每年發現的新勒索軟體數在 2015 年創空前新高，高達 100 個。攻擊者今日要求的平均贖金已躍升至 679 美元。

對企業的攻擊正逐漸增加。雖然大規模、無差別攻擊的勒索軟體活動仍是最普遍的威脅形式，但也出現更新和更先進的攻擊。越來越多網路犯罪組織開始鎖定攻擊大型企業。本報告中的兩個案例研究顯示，這些攻擊涉及高階專業技術，利用網路間諜活動中常見的技術，入侵並周遊於目標網路中。

雖然執行方式越來越複雜與耗時，但若能順利鎖定企業，這次攻擊即可影響數千台電腦，造成大規模的營運中斷，以致嚴重損害營收與商譽。一旦網路犯罪組織看見企業屈服於這些攻擊且支付贖金，將有更多的攻擊者群起仿效，企圖奪取潛在利潤。

企業需要充分明白勒索軟體造成的威脅，並優先建立自己的防禦機制。僅管採用多層式安全方法，可將感染的機會降至最低，但是教育一般使用者認識勒索軟體，並鼓勵他們採取最佳實務準則，也是極為重要。因為勒索軟體組織仍不斷地改善犯罪手法，企業切勿過於自滿。企業在面對快速演化的威脅時，應持續審視與改善企業安全。

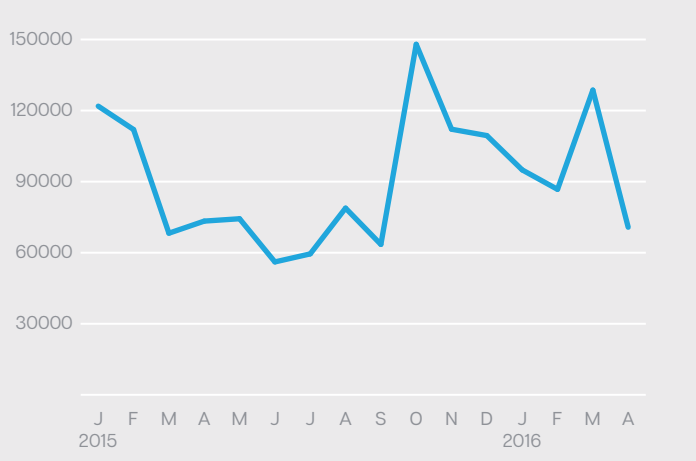
重要發現

- 雖然到目前為止，勒索軟體大多屬於無差別攻擊，但證據顯示，攻擊者對於利用目標式攻擊來襲擊企業越來越感興趣。
- 數個勒索軟體集團已開始利用先進的攻擊技術，展現出許多網路刺探攻擊中所見到的類似專業技術。
- 服務業，佔企業感染的 38%，是目前為止受影響最嚴重的產業。製造業受感染比例為 17%，金融、保險及不動產和公共行政業各佔 10%，比例同樣驚人。
- 平均贖金要求從 2015 年底的 294 美元躍升到今日的 679 美元，已翻漲超過一倍。
- 自 2011 年以來，發現的全新勒索軟體數已逐漸增加。去年創下歷史新高，共發現 100 個全新勒索軟體。
- 勒索軟體即服務 (RaaS) 的出現，表示眾多網路罪犯可取得自己的勒索軟體，包括專業技術相對較低的網路罪犯。
- 持續轉向加密型勒索軟體。2016 年到目前為止，只發現一支全新勒索軟體，其餘都是加密型勒索軟體，與去年相較之下，大約佔了 80%。
- 從 2015 年 1 月到 2016 年 4 月這段時間，美國是全球勒索軟體肆虐最嚴重的地區，佔全球感染量的 28%。加拿大、澳洲、印度、日本、義大利、英國、德國、荷蘭及馬來西亞，分別位居 2 至 10 名。約有 43% 的勒索軟體受害者，是企業組織內的員工。

勒索軟體概述

勒索軟體在 2015 年第一季的攻勢稍見緩和之後，到了第四季整體感染數字又開始攀升，在十月、十一月及隔年三月，感染記錄更是屢創新高。2016 年 3 月的感染高峰，正好與 Locky 這款惡意勒索軟體 (Trojan.Cryptolocker.AF) 的出現落在同一時期。

圖 1. 從 2015 年 1 月到 2016 年 4 月每月發生的勒索軟體感染總數



加密型勒索軟體的崛起

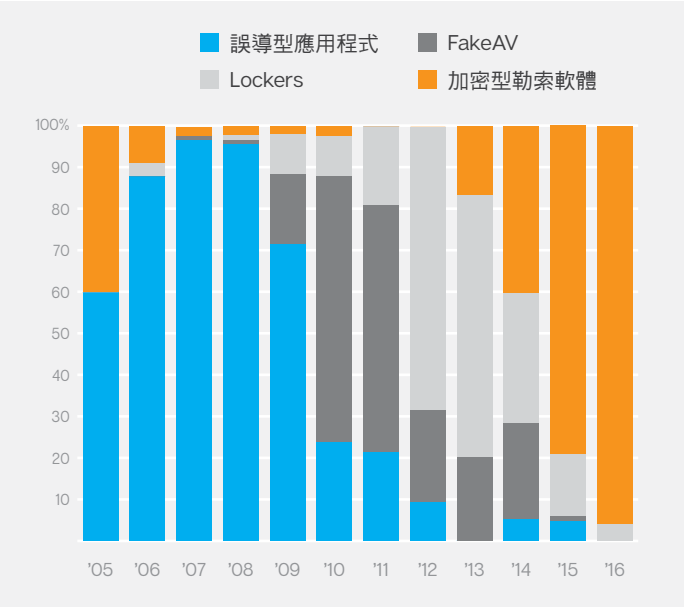
最近幾年來，加密型勒索軟體有逐漸崛起的趨勢。 在最新勒索軟體白皮書中，我們注意到歸類為加密型勒索軟體的最新變種比例已逐年增加。這個趨勢持續到 2016 年，今年到目前為止，賽門鐵克只記錄一支全新的勒索軟體，其餘都是加密型勒索軟體。

七到十年前，誤導型應用程式稱霸市場，許多誤導型應用程式會偽裝成防毒軟體。這些風險會告知使用者電腦出問題，例如感染惡意程式或軟體有問題。攻擊者則要求支付款項來「修復」問題。

之後，鎖定型威脅會隱匿偽裝的防毒應用程式。Locker 會阻止存取感染的裝置，但不會加密或刪除任何檔案。移除惡意程式之後，通常就可還原裝置的完整存取權限。在 2012 和 2013 年享受了短暫的全盛期之後，鎖定型勒索軟體已逐漸減少，取而代之的是加密型勒索軟體。

加密型勒索軟體之所以會崛起，因為它通常是最有效的勒索軟體。如果建置正確，加密型勒索軟體將會加密使用者檔案，無法破解。移除惡意程式並無法解決問題；使用者仍然無法存取檔案。如果受害者未備份這些檔案，則支付贖金可能是復原檔案的唯一方式。過去兩年來，加密型勒索軟體的運作模式已臻完善，因此在今日能大行其道也不足為奇。

圖 2. 2005 年到 2016 年 6 月間，經確認的全新誤導型應用程式、偽裝防毒軟體、鎖定型勒索軟體，以及加密型勒索軟體的百分比

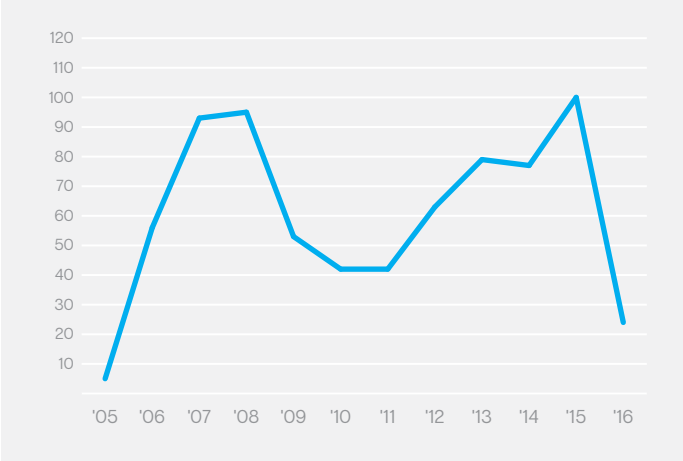


創紀錄的全新勒索軟體數量

近年來加密型勒索軟體的成功，促使全新勒索軟體的大量崛起。2015 年是勒索軟體數量創新高的一年，賽門鐵克發現了 100 支新型的勒索軟體，是至今最高紀錄。

越來越多的網路犯罪集團嘗試利用勒索軟體，欲從中獲利。現在透過勒索軟體建立套件或勒索軟體即服務 (RaaS) 建立自己的勒索軟體也比以往更加容易，因此地下網路罪犯紛紛起而效尤。

圖 3. 每年發現的全新勒索軟體總數 (2016 年圖表記錄截至 4 月底前發現的全新勒索軟體)

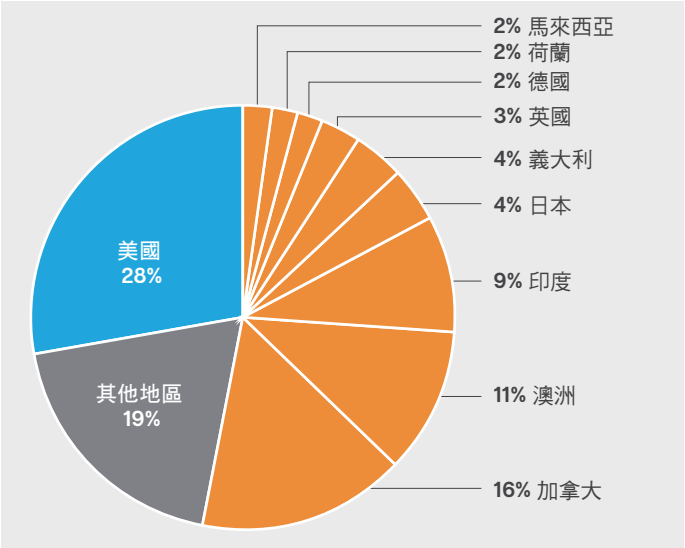


美國一直是遭受勒索軟體感染最嚴重的國家

由於在 2015 年 1 月到 2016 年 4 月記錄的感染數字佔總感染量四分之一強，使得美國繼續蟬聯勒索軟體最猖獗橫行的地區。緊追在後的加拿大 (16%)、澳洲 (11%) 和印度 (9%) 也深受其苦。義大利 (4%)、英國 (3%)、德國 (2%) 及荷蘭 (2%) 等西歐國家的感染統計數字也不可謂不高。其他同樣位居前十名的國家還包括日本 (4%) 和馬來西亞 (2%)。

統計資料表示攻擊者主要針對已開發富裕國家，作為其活動重點目標。

圖 4. 2015 年 1 月到 2016 年 4 月各地區發生的勒索軟體感染總數



最新技術

在過去的這一年裡，勒索軟體攻擊者使用數個最新技術做為武器。攻擊者使用不同的程式語言來撰寫數種新勒索軟體程式碼，例如 JavaScript、PHP、PowerShell，或 Python。攻擊者使用這些語言，達到規避資安產品偵測的目的。

一些知名的勒索軟體，也開始加入鎖定裝置或加密檔案等核心功能以外的功能。例如，CryptXXX (Trojan.Cryptolocker.AN) 中擁有一個額外功能，能取得比特幣錢包資料並將資料傳送給攻擊者。據報，Cerber (Trojan.Cryptolocker.AH) 能將受感染的電腦加入魁儡網路，然後再利用受感染的電腦進行分散式阻斷服務 (DDoS) 攻擊。

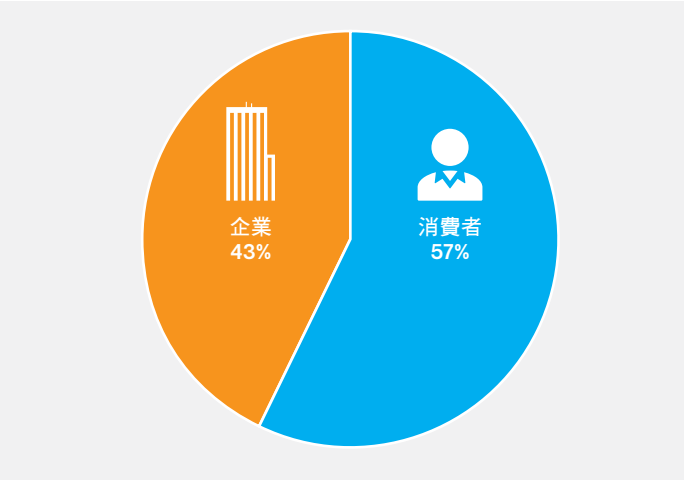
Chimera (Trojan.Ransomcrypt.V) 可在勒索訊息中進行其他威脅。除了加密檔案以外，惡意程式會威脅將受害者的檔案 (包括圖片和影片) 公布在網路上。

這些最新技術的採用展現出勒索軟體的持續演進，以維護其立足之地並保持獲利。

哪些人是受害者？

消費者是勒索軟體最有可能的受害者，在 2015 年 1 月到 2016 年 4 月之間所有感染總數中佔了 57%。雖然大多數主要勒索軟體集團傾向進行無差別攻擊，但是消費者往往不太可能具備穩固的安全防護，因而提高了淪為勒索軟體受害者的可能性。

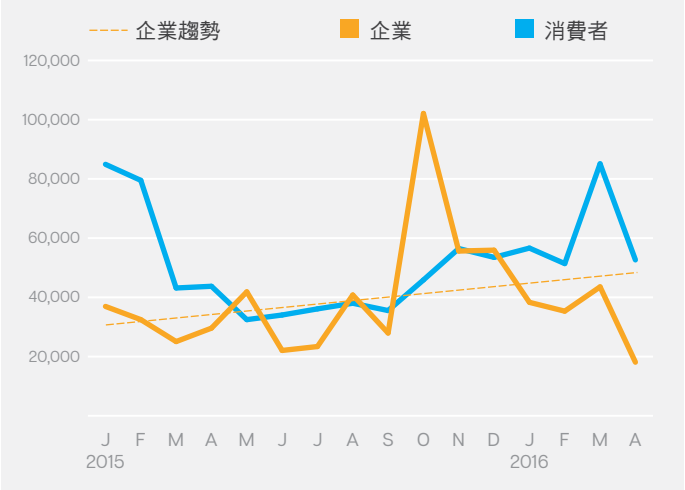
圖 5. 2015 年 1 月到 2016 年 4 月消費者與企業發生的勒索軟體感染總數比較



在 2015 年初，受感染的消費者比例比受感染的企業超過一倍以上。受感染的消費者人數在 2015 年第一季下降，而這兩個目標類型在第一季後的分析數字大約相等。由於受感染的企業數激增，2015 年 10 月的數字卻掉出趨勢之外。仔細查看每月統計數字後會發現，企業受勒索軟體攻擊的長期趨勢穩定而緩慢地上升。

儘管趨勢如此，2016 年第一季的消費者感染總數又再次超越企業感染總數。由於沒有證據顯示攻擊者將更多攻擊目標鎖定在消費者上，對最近幾個月感染趨勢變化的解釋是，企業對於勒索軟體的危機意識正在提升。例如 TeslaCrypt (Trojan.Cryptolocker.N) 與 Locky 等威脅在 2015 年底和 2016 年初，皆透過大量的垃圾郵件活動廣泛地散播，許多企業在這次垃圾郵件衝擊中受到波及。對安全性越注重，表示能盯上企業電腦的勒索軟體酬載就越少。

圖 6. 2015 年 1 月到 2016 年 4 月消費者與企業每月發生的勒索軟體感染總數比較



哪種類型的企業最有可能受感染？

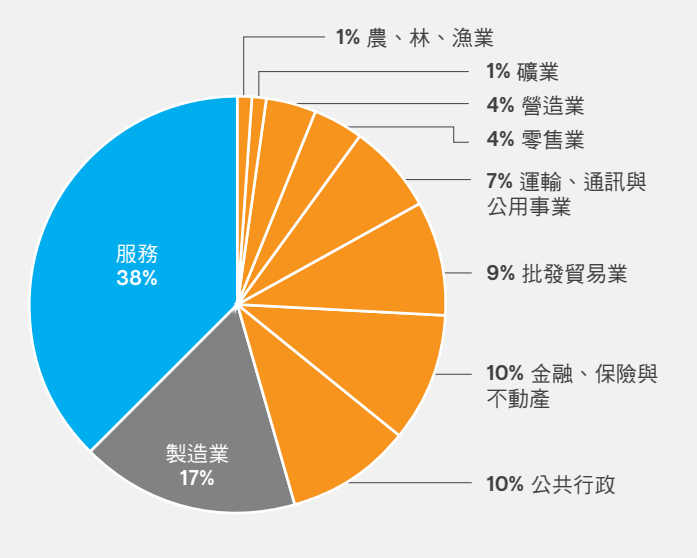
近年來，幾乎各行各業都受到勒索軟體的影響，但是某些類型的企業似乎較容易受到攻擊。在分析已受感染的產業之後發現，2015 年 1 月到 2016 年 4 月之間，服務業受感染的比例為 38%，是迄今受到勒索軟體影響最鉅的產業。

製造業受感染比例為 17%，金融、保險及不動產和公共行政業各佔 10%，比例同樣驚人。前 10 名為批發貿易業 (9%)、運輸、通訊和公用事業 (7%)、零售業 (4%)、建築業 (4%)、礦業 (1%)，以及農林漁業 (1%)。

迄今尚不清楚，為什麼某些產業比其他行業更容易受感染。其中一個可能的解釋是，與不同網際網路服務緊密整合的企業較容易暴露在感染風險中，因此服務業受感染總數高於其他產業。

儘管最近幾個月醫療保健業傳出的攻擊事件層出不窮，但醫療保健業並未列在最常受感染的產業。原因是，最近知名的醫療保健攻擊多數屬於目標式攻擊。雖然會對受感染企業造成嚴重損害，但這類攻擊的攻擊頻率相對來說不高，因此整體感染統計數字仍是由大規模無差別攻擊中所使用的勒索軟體變種所主導。如需深入瞭解目標式攻擊，請參閱下列章節：企業：下一個重要目標。

圖 7. 2015 年 1 月到 2016 年 4 月各產業發生的勒索軟體感染總數



推動成長與持續的因素

加密型勒索軟體市場在過去兩年已趨於成熟狀態。勒索軟體運作模式的完善由幾個關鍵因素促成。

加密

其中一個主要的成長趨動力是可輕鬆取得的強式加密功能，有助惡意行動者製造強大的威脅。攻擊者必須克服的其中一項主要障礙是如何有效地部署加密，而近年來已有大幅進展。

加密型勒索軟體的早期變種常有明顯的設計缺陷。這些瑕疵包括在受感染的電腦上留下加密金鑰，或在所有感染使用相同的加密金鑰，這表示取得金鑰的人可與其他受害者共用金鑰。雖然這些瑕疵仍然發生，但已經非常少見。最新的勒索軟體會針對每一個感染產生新的專屬金鑰。

許多近期的勒索軟體運用混合的對稱式和非對稱式加密。對稱式加密使用相同的私密金鑰來加密和解密檔案。對稱式加密的優點是可以快速加密檔案。這點對攻擊者來說相當重要，因為他們希望在感染被發現之前完成加密。對稱式加密對於攻擊者的缺點是，如果在加密期間金鑰被找到，則受害者就可使用金鑰來解密所有資料。

非對式稱加密使用兩種加密金鑰：公開金鑰與私密金鑰。公開金鑰儲存在受害者的電腦上，用來加密檔案。解密檔案則需要私密金鑰，而私密金鑰存放在遠端位置。這樣雖然比較安全，但是加密過程則緩慢許多。

結合這兩種方法可讓攻擊者善用這兩者的優勢，這也是所有開發人員常見的做法。攻擊者可利用對稱式加密快速加密受害者的檔案，然後採用非對稱式加密來加密對稱式加密金鑰。如此一來，較安全但較緩慢的非對稱式加密，就只需要加密一個檔案。

加密貨幣的出現

贖金支付方式對於網路罪犯而言一向是個挑戰，網路罪犯需要的方式是能輕鬆聯絡受害者、輕鬆兌現，但難以追蹤的方式。攻擊者以前大量採用付款憑單方式。

比特幣和其他加密貨幣崛起後，提供了傳統金融體系以外的贖金支付選擇。雖然不是完全匿名的方式，但比特幣透過各個錢包和洗錢服務來移動，使得比特幣的動向隱晦不明。比特幣錢包是免費而且可拋棄的，表示攻擊者可以為每個感染產生全新的專屬錢包，讓執法人員難以追查所有收入。

比特幣廣為大眾所知，也意味著受害者對加密貨幣較不存疑，因此可能會購買比特幣來支付贖金。某些勒索軟體曾嘗試使用網路商店的禮品卡作為支付贖金的方式，例如 iTunes 儲值卡，但不是很成功，因為容易被追蹤且難以兌現。

有效的感染媒介

開發出有效勒索軟體對攻擊者而言只成功了一半。他們也需要確保勒索軟體能擴散到更多使用者。去年出現一些勒索軟體集團，例如 TeslaCrypt 和 Locky，執行主要的垃圾郵件活動。導致數百萬使用者幾乎每天都遭受攻擊。即使只有少部分使用者受到感染，隱藏在這些危害背後的攻擊者很可能會獲得豐厚的利潤。

除此之外，也發現到幾個主要的刺探套件正在散佈勒索軟體。例如，在最近幾個月來，Angler 刺探套件是 CryptXXX 的其中一個主要傳遞管道。也發現到 Neutrino 刺探套件正推動數個勒索軟體變種，包括 Locky、Cerber，以及 CryptoWall (Trojan.Cryptowall)。

先進的攻擊技術

數個勒索軟體集團開始採用先進的攻擊技術，對企業進行目標式攻擊。這些攻擊運用的專業技術與在許多網路刺探攻擊中所見的雷同。攻擊者在找出並感染數百台電腦之前，會先設法利用公開網頁伺服器中的漏洞，然後使用合法工具周遊在網路之間，取得立足點。進行此類攻擊所需的時間和技術遠超過進行標準勒索軟體攻擊活動，但是能獲得的報酬更多。

勒索軟體即服務

RaaS 的興起，讓原本無法利用勒索軟體的人，都能進入勒索軟體的領域。現在，即使是技術程度不高的人也可以購買勒索軟體執行檔來存取使用者介面，追蹤受害者。RaaS 建立者只要坐著等客戶散佈惡意程式，就可以從中賺取利潤。

感染媒介

勒索軟體運用多種方式來感染電腦，某些方式較其他方式普遍。

惡意電子郵件

其中一個用來散佈勒索軟體與惡意程式的常見方法是透過惡意垃圾電子郵件。此垃圾郵件利用傀儡網路 (受感染電腦的網路) 來散佈，受感染的電腦數從數百台到數百萬台都有。傀儡網路利用社交工程戰術發送大量垃圾電子郵件，誘騙收件者洩漏自己電腦中的資訊。如果使用者執行以下任意一項動作，就可能受到感染：

- 開啟會直接安裝勒索軟體的惡意附件
- 開啟惡意附件，透過下載程式 (通常是巨集) 起始第二階段傳送，隨後下載並安裝勒索軟體
- 按下指向刺探套件的連結，導致在電腦上安裝惡意程式

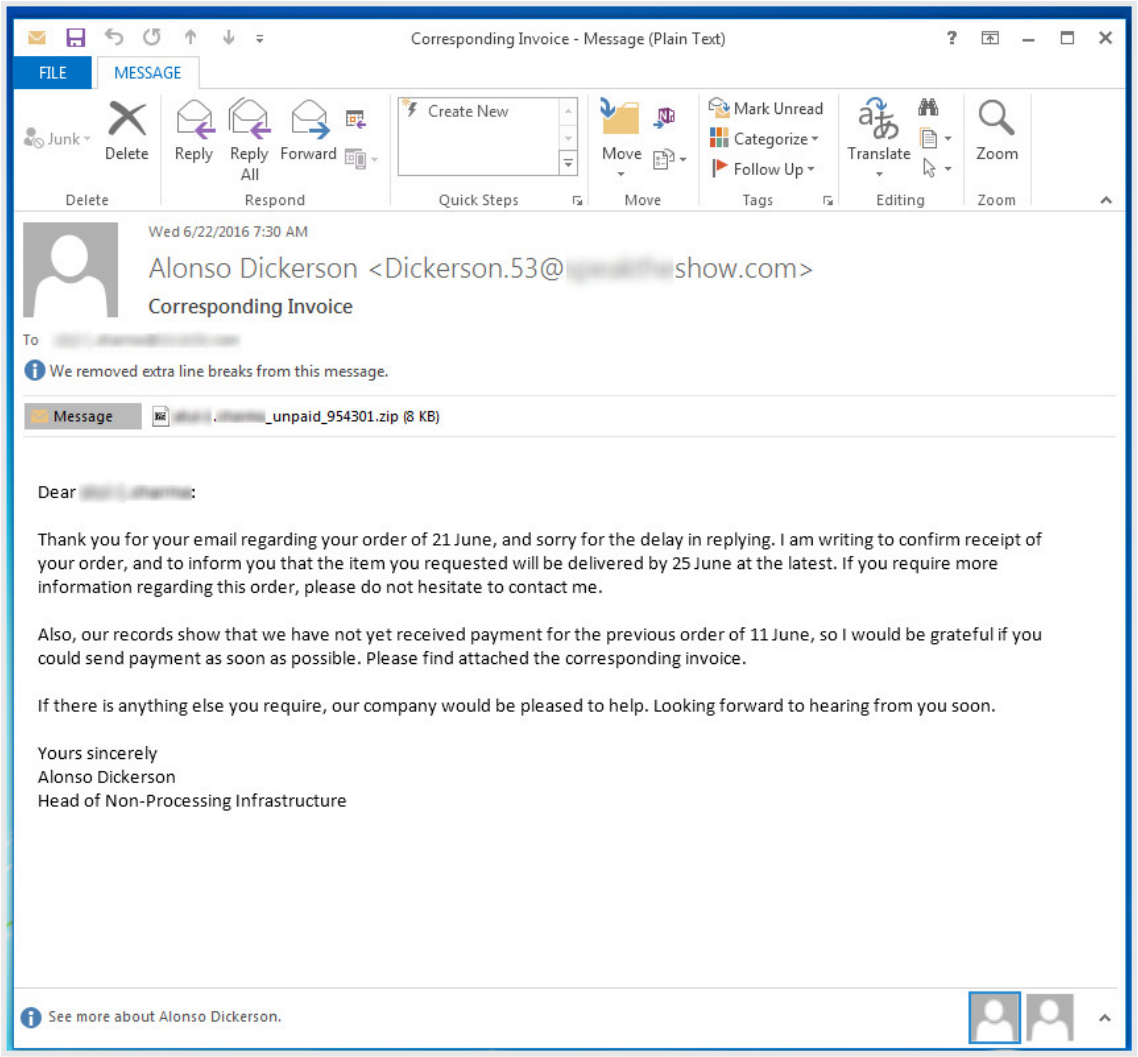
用於散佈勒索軟體的垃圾郵件經常偽裝成來自知名企業的重要電子郵件，例如：

- 來自郵局或其他貨運公司的通知，通知收件者收貨
- 來自公用事業供應商的逾期帳單通知
- 收件者的退稅提醒
- 商品及服務的發票
- 假冒信用卡獎勵計劃

每個垃圾郵件變種都在利用使用者的既有直覺，讓他們針對那些看起來緊急的郵件採取行動。

圖 8 顯示典型的發票垃圾郵件範例。在與垃圾郵件對戰的過程中，賽門鐵克已攔截超過 500,000 封散佈 Locky 的惡意電子郵件。雖然這個攔截數量在勒索軟體垃圾郵件活動中實為常見，但有時攔截的電子郵件數目還會達到上百萬封之多。

圖 8. 垃圾電子郵件散佈 Locky 的範例



攻擊者運用各種手段，透過垃圾電子郵件有效散播勒索軟體。例如今年初，有些攻擊者使用 Windows 指令檔 (WSF) 來略過電子郵件過濾。具有 .wsf 副檔名的檔案可像執行檔一樣啟動。一旦開啟了電子郵件附件 (包含 .doc 檔案的壓縮資料夾)，便會執行 .wsf 檔案，將 CryptoWall 安裝在受害者的電腦上。

我們也發現完全由 JavaScript 組成的勒索軟體，透過偽裝成 .doc 檔案的垃圾郵件附件傳播。惡意附件開啟後，JS.Racryptor (又稱為 RAA)，會立即開始加密檔案。JavaScript 並非首次被運用在勒索軟體活動中。Ransom32 (Trojan.Ransomcrypt.Y) 使用 NW.js，它是一種使用 JavaScript、用來開發 Windows、Linux 和 Mac OS X 桌面應用程式的架構。不過，雖然 Ransomware32 封裝成執行檔，JavaScript 檔案仍會單獨傳送 RAA。

垃圾郵件容易執行，且依賴社交工程，而非先進技術，因此仍是散播勒索軟體最普遍的方法之一。藉由傳送大量的垃圾電子郵件，攻擊者可在短時間內接觸到為數眾多的受害者。攻擊者不管是使用 .wsf 檔案等新戰術，甚至是故技重施採用惡意巨集，都告訴我們無論郵件看起來有多麼無害，使用者和企業在處理電子郵件時，務必謹慎小心。

阻止惡意電子郵件必須採用多種方式，包括使用電子郵件掃描服務，以及教育使用者使用電子郵件的最佳實務準則。Symantec Email Security.cloud 與 Symantec Messaging Gateway 可阻絕惡意程式、惡意網址，以及網路釣魚等電子郵件威脅，讓這些威脅無從接觸使用者。這兩項產品也會使用程式碼分析和模擬，找出並攔截電子郵件內的惡意 JavaScript。

刺探套件

刺探套件 (Exploit kit，簡稱 EK) 是勒索軟體另一種普遍的感染媒介。 這些工具組利用軟體中的漏洞來安裝惡意程式。刺探套件攻擊者會入侵第三方網頁伺服器，並將 iframe 植入在這些伺服器上執行的網頁。iframe 會將瀏覽器導向刺探套件伺服器。

攻擊者可利用下列方式將使用者重新導向到刺探套件：

- 垃圾電子郵件或社交媒體貼文中的惡意連結
- 惡意廣告
- 來自流量分散服務的重新導向網頁流量

使用這些套件的犯罪分子利用使用者電腦上過時或未修補的軟體，但不幸的是，潛在目標為數眾多。賽門鐵克每天從所有刺探套件攔截到的攻擊數量多達 120 萬個。

刺探套件的操作者偏愛零時差漏洞，因為這些未經修補的漏洞可提供最高的投資報酬率。套件操作者與軟體開發人員正進行不斷的競賽，務必要在漏洞經修補之前，整合新的攻擊方法。Angler EK 一直引領群雄，直到 2016 年 6 月才驟然消失。 2015 年，賽門鐵克光從 Angler 就攔截了 1950 萬次攻擊。Angler 大多利用 Adobe Flash 中的漏洞，其中 64% 的攻擊主要針對 Windows 7 電腦。

網路罪犯可能會付錢給刺探套件操作者，請他們散佈勒索軟體。因此，每個套件帶來的威脅會隨著時間而改變。根據我們的資料顯示，2016 年 5 月散佈最多 CryptXXX 勒索軟體的分屬 Angler 和 Neutrino 刺探套件。Neutrino 和 Magnitude 則是散佈 Cerber。Rig 散佈 Cerber 和 Locky。

不過，網路罪犯世界瞬息萬變，2016 年 6 月我們發現發動 Locky、Dridex、Angler 和 Necurs (Backdoor.Necurs) 攻擊的數個知名網路犯罪集團活動數量忽然驟降。賽門鐵克遙測技術發現這些威脅都大幅減少活動，或在這段時間內完全沒有任何活動 (雖然 Locky 目前已再度浮上檯面，而除了 Angler 以外的其他威脅也開始恢復活動)。

在俄羅斯逮捕涉嫌銀行詐騙的網路罪犯之後的同一時間，攻擊活動也同時減少，不過減少的原因仍然是個謎。儘管涉嫌的網路罪犯和造成影響的威脅之間沒有已知的關聯，但是 Locky、Dridex、Angler 和 Necurs 集團可能利用執法行動中遭關閉或查獲的基礎架構。類似事件顯示出威脅態勢的快速變化，以及若要保持領先必須擁有可靠的情報。

賽門鐵克最近發現，偽裝成技術支援的詐騙者將受害者重新導向到刺探套件，散播勒索軟體。詐騙者嘗試欺騙受害者付費修復不存在的電腦問題，以進行常見的技術支援詐騙。但是，詐騙者同時會將使用者重新導向到服務 CryptoWall 的 Nuclear 刺探套件。

雖然過去曾經發現技術支援詐騙使用勒索軟體技術，但我們首次發現他們使用實際的勒索軟體。技術支援詐騙者會嘗試各種方式，提高向受害者成功索錢的機率。或者，詐騙者本身可能是另一個攻擊的受害者。刺探套件操作者可能在此次活動中入侵詐騙者的伺服器，以傳送自己的勒索軟體。

其他感染媒介

雖然電子郵件和刺探套件是用來散播勒索軟體的兩種主要方法，但還有下列技術：

惡意廣告： 惡意廣告刊登到廣告聯播網上，以借其之力出現在社會大眾所信任、擁有大量訪客的網站上。 在某些情況下，訪客甚至不用點選廣告，只要載入擁有惡意廣告的網頁就會造成感染，且通常是透過重新導向到刺探套件造成感染。廣告的惡意元件存在時間短暫，移除惡意廣告後，惡意元件即消失無蹤。勒索軟體罪犯之所以會使用惡意廣告，原因是可透過即時廣告競標網路購買廣告空間，因此可輕鬆鎖定位於經濟富裕地區的人們。

其他惡意程式：勒索軟體也可能透過其他惡意程式進入受危害的電腦。其中一個惡意程式就是惡名昭彰的 Dridex 傀儡網路，以收集銀行憑證著名。在某次掃蕩行動中逮捕到其中一位 Dridex 傀儡網路操作者，傀儡網路雖在某種程度被終止，但很快就重振旗鼓。Dridex 傀儡網路細分成數個子網路，可能由不同人操作。掃蕩過後不久，其中一個子網路不再發送包含 Dridex 的垃圾郵件，轉而散佈包含下載程式的垃圾郵件，而該下載程式會下載 Locky。還可以使用 Bot 傀儡程式安裝勒索軟體，企圖盡最後努力從受感染的電腦獲利。

強制破解密碼：散播勒索軟體的新興策略是強制破解伺服器上所使用的軟體登入憑證。Bucbi 勒索軟體 (Trojan.Ransomcrypt.AO) 背後的犯罪份子利用此方法，在遠端桌面通訊協定 (RDP) 伺服器上取得立足點。此威脅會加密 RDP 伺服器可存取之電腦和其他伺服器上的檔案。

攻擊伺服器漏洞：近來發現攻擊者鎖定伺服器上執行的軟體漏洞，以取得企業網路的存取權限。SamSam 勒索軟體 (Trojan.Ransomcrypt.AE) 背後的集團使用免費的工具來尋找、入侵漏洞，將惡意程式散播到整個網路。

去年，Linux.Encoder (Unix.Ransomcrypt) 勒索軟體和 CTB-Locker (Trojan.Cryptolocker.G) 新變種也相繼問世。Linux.Encoder 主要針對 Linux 作業系統，目標是部署網頁伺服器的電腦。攻擊者藉由攻擊網站外掛程式或第三方軟體中的漏洞，來感染受害者。然後 Linux.Encoder 會加密與網站檔案相關的目錄，造成受感染電腦上所控管的網站無法使用。

自行傳播：雖然我們已經發現 Android 勒索軟體出現類似病蟲的行為，如利用簡訊將勒索軟體散播給裝置通訊錄上所有聯絡人，但是 ZCryptor (W32.Cryptolocker.AQ) 可能是第一個在 Windows 平台上出現自行傳播行為的勒索軟體。ZCryptor 在加密前會先自我複製，感染所有抽取式磁碟機，提高其散播至其他電腦的機會。

簡訊與第三方應用程式商店：如上所述，Andriod 勒索軟體威脅可透過簡訊散播，然而他們也可以透過不受信任的第三方應用程式商店進入裝置。其中一個範例是 Android.Lockdroid.E，它會偽裝成第三方應用程式商店中的色情影片播放程式。這個應用程式不但不會播放成人影片，相反地，它會利用裝置相機拍攝受害者照片，並將照片放入勒索信中。

受到勒索軟體影響的平台

儘管攻擊 Windows 使用者一直是勒索軟體的主流，現在卻出現越來越多針對其他平台的勒索軟體活動。隨著各犯罪集團競相尋找未經入侵的目標對象，這個趨勢很可能會持續下去。

Windows 使用者

同時感染企業與消費者的無差別攻擊活動，是勒索軟體攻擊迄今為止最主要的形式。大多數的攻擊目的只是盡可能感染越多電腦，以獲取最多的報酬。因此，大多數的勒索軟體變種目的在攻擊 Windows 電腦。

Windows 家庭使用者仍是最大的受害者族群。相較於企業，家庭使用者較不可能使用安全軟體，也不可能保存寶貴資料的最新備份，因此他們的電腦較容易遭受攻擊。雖然家庭使用者付不出龐大的贖金，但是因為潛在受害者人數眾多，代表他們仍是相當有利可圖的目標。

攻擊家庭使用者的同一個勒索軟體，同樣也會對企業造成影響。如果企業未受到保護，後果可能不堪設想。一台受感染的電腦，家庭使用者可能只需付出 500 美元的贖金，但是對於一家企業，為多部受感染電腦所需支付的贖金則會急遽增加到上萬美元。

除了這些大規模的攻擊之外，勒索軟體集團現在逐漸偏好利用自訂攻擊來鎖定企業 (請參閱：企業：下一個重要目標)。

行動裝置使用者

由於智慧型手機的普及，可想見亟欲入侵這些裝置的勒索軟體攻擊者越來越多。近幾年出現的數個 Android 威脅，絕大部分是鎖定型威脅。然而，俄文的 Simplocker (Android.Simplocker) 與其英文變種 (Android.Simplocker.B) 則是針對 Android 裝置的新興加密型勒索軟體。

雖然目前沒有專門針對 iOS 的勒索軟體記載案例，但是網頁式變種也會影響到 iOS 裝置。

Mac OS X 使用者

直到最近，勒索軟體集團才開始針對 Mac OS X 使用者。2016 年 3 月，稱為 KeRanger (OSX.Keranger) 的威脅成為第一個針對 Mac OS X 作業系統，且廣泛散佈的勒索軟體。KeRanger 散佈在受感染的 Transmission BitTorrent 用戶端安裝程式中。

KeRanger 的行為類似現代的 Windows 勒索軟體，它會先搜尋並加密大約 300 個不同的檔案類型，之後再要求 1 枚比特幣 (本報告撰寫當時為 678 美元) 的贖金。

惡意程式具有有效的 Mac 開發人員 ID 簽章。這表示 KeRanger 可略過 Mac OS X 的 Gatekeeper 功能，這個功能用來攔截來自未受信任來源的軟體。Apple 會快速撤銷 KeRanger 使用的開發人員 ID。

在此之前，2015 年 11 月，巴西的網路安全研究人員 Rafael Salema Marques 開發出一套概念證明 (PoC) 勒索軟體，稱為 (OSX.Ransomcrypt)。Marques 此舉的目的在突顯出 Mac OS X 電腦無法免於勒索軟體的威脅。

未來目標

隨著物聯網 (Internet of Things，簡稱 IoT) 的成長，可能受勒索軟體感染的裝置種類隨之倍增。當人們逐漸意識到勒索軟體對傳統電腦的影響，攻擊者即可能會轉向物聯網，尋找更容易攻擊的新目標。

例如，Android 勒索軟體 Flocker (Android.Lockdroid.E) 可鎖定 Android 智慧型電視。最新版 Flocker 要求受害者支付 200 美元的 iTunes 禮品卡作為贖金。賽門鐵克研究人員 Candid Wueest 去年即預測到這類攻擊的發生，他曾經針對智慧型電視示範一次成功的勒索軟體攻擊。

圖 9. 受到勒索軟體感染的智慧型電視

智慧型手錶是另一個潛在的攻擊途徑。去年，賽門鐵克針對 Android Moto 360 智慧型手錶，示範了一次成功的概念證明勒索軟體攻擊。

另一個令人擔憂的潛在目標是工業控制系統 (ICS)。已出現惡意程式對於 ICS 裝置發動攻擊的案例，其中最著名的是 Stuxnet。有鑑於最近興起的目標式勒索軟體攻擊，以及 ICS 攻擊可能造成的中斷情況，攻擊者早晚會將注意力轉向工業控制系統。如果攻擊者利用勒索攻擊來中斷製造過程，將會帶來破壞性的影響。

主要的勒索軟體

勒索軟體態勢不斷變化，每個月都有全新的勒索軟體出現。除了最新威脅的崛起，舊有的勒索軟體也可能會隨著它們的興起而消失。TeslaCrypt 就是一個明顯的例子，它是 2015 年底到 2016 年初其中一個散播最廣的勒索軟體變種。2016 年 5 月，集團突然停止運作這個勒索軟體，並發佈通用解密金鑰。攻擊者在他們的 Tor 網站上宣布一個簡明扼要的消息，說明該計劃已「結束」，並寫下「我們深感抱歉」具結。

以下是本報告撰寫當時，最普遍的加密型勒索軟體威脅：

Cerber

偵測名稱：Trojan.Cryptolocker.AH

贖金金額：1.24 到 2.48 枚比特幣 (以 2016 年 3 月的匯率計算為 513 到 1,026 美元)

發現時間：2016 年 3 月

已知的感染媒介：垃圾郵件活動、Neutrino 刺探套件、Magnitude 刺探套件

圖 10. Cerber 勒索信，通知使用者檔案已遭到加密，並提供使用者如何解密檔案的說明

Cerber 是勒索軟體中最新進的威脅，從 3 月問世以來，即已造成嚴重的影響。Cerber 與 Locky 類似，可存取 Dridex 垃圾郵件網路，這表示可藉由大型垃圾郵件活動快速散播。某些主要刺探套件也可散播 Cerber。Cerber 其中一個新功能是利用語音轉文字 (TTS) 模組，向受害者朗讀勒索信。

CryptXXX

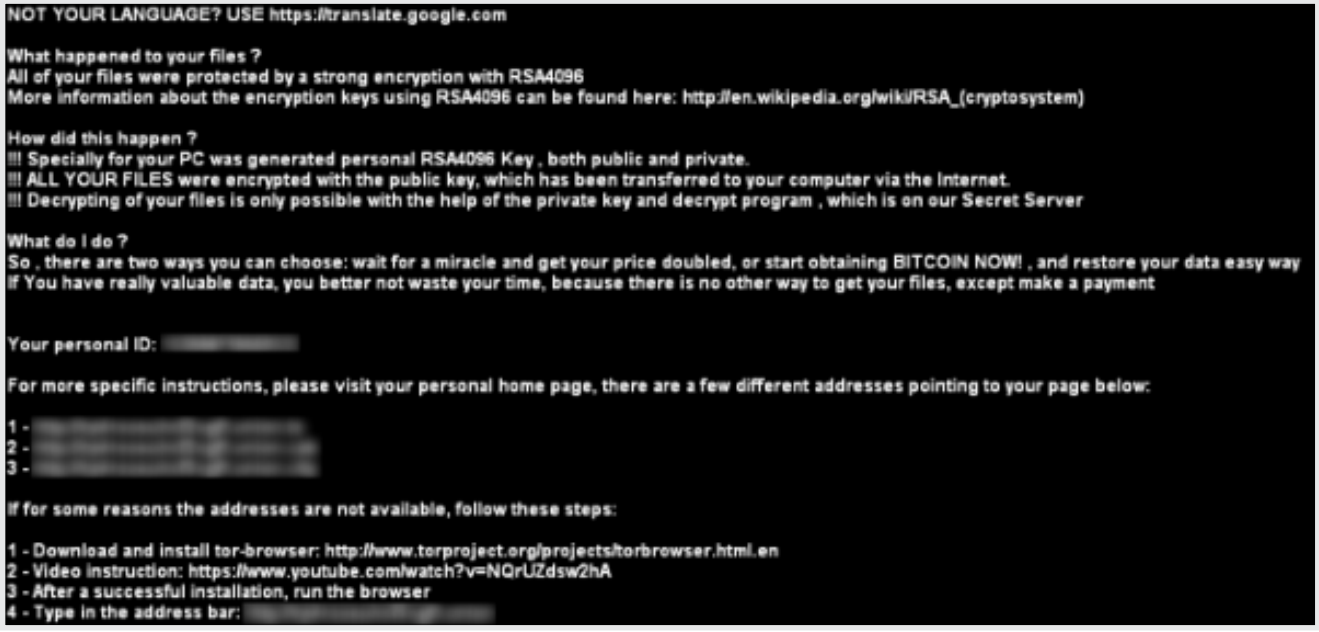
偵測名稱：Trojan.Cryptolocker.AN

贖金金額：500 美元的比特幣

發現時間：2016 年 4 月

已知的感染媒介：Angler 刺探套件、Neutrino 刺探套件

圖 11. CryptXXX 勒索信，告知使用者檔案已遭到加密，要求付款以解密檔案



據報是由 Reveton (Trojan.Ransomlock.G) 背後的同一位攻擊者所開發，CryptXXX 在 2016 年 4 月首次出現，之後幾星期內即四處散佈。CryptXX 近來主要由受感染的網站散播，將使用者重新導向到 Angler 刺探套件。這些與 Angler 相關的攻擊會先將 Trojan.Bedep 置入受感染的電腦中。然後 Trojan.Bedep 會利用 CryptXXX 感染電腦。

Angler 刺探套件在 6 月初的消失，預告 CryptXXX 活動的沒落。然而威脅卻又再度出現，目前透過 Neutrino 刺探套件散播。

CryptXXX 一開始的變種使用弱式加密，因此安全研究人員得以為遭到入侵的電腦建立解密工具。但是，攻擊者快速地因應，在惡意程式的最新變種中採用更強的加密方法，解密工具因此失效。

CryptXXX 擁有可收集比特幣錢包資料的功能，並可將資料傳送給攻擊者。

Locky

偵測名稱：Trojan.Cryptolocker.AF

贖金金額：0.5 到 1 枚比特幣 (以 2016 年 2 月的匯率計算為 200 到 400 美元)

發現時間：2016 年 2 月

已知的感染媒介：垃圾郵件活動、Neutrino 刺探套件、Nuclear 刺探套件

圖 12. Locky 勒索信，告知使用者檔案已遭到加密，並提供取得解密程式的說明

自從 2016 年 Locky 的興起到現在，Locky 已創下至今最多勒索軟體變種的歷史紀錄。Locky 背後的攻擊者會透過 Dridex 金融木馬程式所使用的相同垃圾郵件網路來散播威脅。攻擊者因此可傳送大量內含勒索軟體的垃圾郵件。Locky 也會透過數個刺探套件來散佈。

Locky 集團最近開始在垃圾郵件活動中，使用稱為 Rockloader (Downloader.Zirchap) 的最新下載程式。受害者會先感染 Rockloader，然後再將 Locky 下載到電腦中。

6 月初，Locky 的活動驟降，引發人們臆測是否它會永久消失。不過，經過約三個星期的平靜期之後，散播 Locky 的垃圾郵件活動又再次展開。

企業：下一個重要目標

網路罪犯意識到企業帶來的高利潤後，即開始鎖定更多企業為攻擊目標。在其他攻擊活動中同樣發現到這項趨勢，例如：

- 商務電子郵件攻擊 (BEC) 詐騙活動，試圖詐騙高階主管，轉出大筆金額
- 漏洞狩獵攻擊，攻擊者入侵企業伺服器、竊取資料 (作為入侵證據)，並要求支付費用方能獲得攻擊進行方式的資訊
- Carbanak 組織，直接以銀行為目標，而非銀行客戶

勒索軟體組織已成為最新的潮流趨勢。向企業勒索贖金可大幅提高攻擊者的投資報酬率。近來，賽門鐵克發現受勒索軟體鎖定的企業逐漸增加。多數新受害者是因為員工開啟了惡意垃圾電子郵件或造訪惡意網站，而受到無差別攻擊活動攻擊。然而，遭受更危險的目標式攻擊的受害者正不斷增加。

許多目標式勒索軟體攻擊使用的手法類似進階持續性威脅 (APT)，例如：

- 使用可免費取得的工具，一邊取得立足點，一邊在網路中移動
- 取得系統管理員憑證，並使用憑證進行橫向移動
- 展開偵查以獲得資訊，幫助犯罪份子向目標企業勒索金錢

在先前的勒索軟體報告中，賽門鐵克就指出這個新興趨勢的初兆。某些案例可追溯到 2012 年，當時有幾家澳洲企業受到加密型勒索軟體的感染，需支付 5,000 元澳幣 (3,700 美元) 才能解密檔案。其中一家澳洲企業是醫療中心，也許這是個初兆，因為當時全球有好幾家醫療中心皆感染勒索軟體。

去年許多新聞報導指出，勒索軟體已感染多家醫院和醫療中心網路、加密檔案，並挾持資料勒索贖金。某些案例是大規模無差別攻擊活動的受害者，某些案例則是特定的目標式攻擊。隨著這類攻擊的興起，促使 FBI 以及美國與加拿大政府向企業發出有關勒索軟體的警報。

案例研究：進階勒索軟體攻擊分析

賽門鐵克資安事端應變中心最近協助大型企業應變勒索軟體疫情。勒索軟體已散佈到上百台電腦、加密用戶端資料，造成重要系統離線。調查顯示，比起一般網路罪犯活動，勒索軟體攻擊與 APT 型攻擊有更多共通性。

罪魁禍首

賽門鐵克調查人員採取的第一步，是在攻擊中找出以 SamSam 變種呈現的勒索軟體，這個勒索軟體專門以鎖定企業著稱。利用 Symantec Endpoint Protection (SEP) 完整掃描客戶的網路，即可顯示感染的程度，並找出所有遭受入侵的電腦。

滲透

賽門鐵克調查人員策劃讓電腦受到感染，進而發展出數個調查線索，瞭解整個攻擊態勢。賽門鐵克團隊發現，攻擊者一開始的入侵點是公開的網頁伺服器。攻擊者透過未修補的漏洞入侵此網頁伺服器。這個漏洞讓攻擊者在受害者網路上擁有立足點。

橫向移動

入侵之後，攻擊者會使用數個可公開取得的工具 (例如 Microsoft Sysinternals 公用程式) 周遊於受害者網路中。由於藉由合法工具周遊於受害者網路，因此在攻擊完成前，將很難偵測到攻擊者。這是進階攻擊常用的技巧。這些工具可讓攻擊者對應企業網路中每台可存取的電腦，鎖定最有價值的資產。

酬載與贖金

找到目標電腦後，攻擊者會利用名為 f.bat 的批次程序檔，在每台電腦上部署 SamSam 和公開加密金鑰。程序檔也會刪除電腦上的磁卷陰影複製，以致無法在感染後還原任何檔案。之後，攻擊者會散佈名為 sqlsrvtmg1.exe 的工具。這個執行檔會搜尋任何正在執行的備份處理程序，並停止備份處理程序。它也會刪除找到的所有相關備份檔案。

感染過程的最後一步是散佈另一個名為 reg.bat 的批次程序檔。這個批次程序檔會在每一台受感染的電腦上啟動加密程序。SamSam 的設定可加密上百種不同的檔案類型。加密程序完成後，勒索軟體會自行刪除，在桌面上留下加密的檔案與勒索信。勒索信會指示受害者造訪某個網站，然後為每台受感染的電腦支付 1.5 比特幣的贖金 (本報告撰寫當時為 989 美元)。

修復與還原

利用 SEP 行為與檔案型特徵，賽門鐵克資安事端應變中心可抑制並根除疫情。一開始的修復作業是確認和刪除所有加密檔案。接著，賽門鐵克資安事端應變中心會從備份資料還原未加密的檔案，而這是個漫長的過程。在某些情況下，使用者未遵守公司政策，如將檔案儲存在本機電腦而未儲存在規定的檔案伺服器上，表示這些檔案未經備份，因此將永久遺失。提供軟體的廠商會重新建置確認為初始入侵點的伺服器。

學到的教訓

這份調查顯示出勒索軟體感染不再只是隨機的大規模攻擊。網路罪犯目前採用一般在進階間諜攻擊才會看到的技術，並利用這些技術鎖定勒索軟體感染的目標。這表示網路罪犯已趨於成熟，企業也儼然成為網路罪犯覬覦的目標。

賽門鐵克資安事端應變中心在調查期間，發現到一些有關客戶的重要問題：

1. 公開伺服器上未修補的漏洞讓攻擊者得以進入其網路。立即修補所有重要軟體套件，可降低透過此方式入侵的風險。
2. 使用者未遵守公司政策 (將檔案儲存在本機，而非儲存在檔案伺服器) 是永久遺失資料的主因。既然沒有這些檔案的備份，也就無法還原這些檔案。
3. 雖然所有工作站和伺服器上都已安裝 SEP，但卻未遵守最佳實務準則。SEP 的「應用程式與裝置控制」功能未部署在企業伺服器上，這表示可協助阻止感染擴散的這項重要且有效的工具，無法為客戶帶來好處。

透過賽門鐵克資安事端應變中心的協助，客戶可快速地找出每台受感染的電腦，並防止攻擊者進行任何進一步的危害。確認初始攻擊的來源並找出攻擊者在受害者網路中周遊的方式之後，資安事端應變中心就能提供客戶專屬的行動項目，以加強防禦並阻止進一步攻擊。

鎖定企業的酬載

針對一般使用者的勒索軟體是採用誤打誤撞的方式。在這些活動中，攻擊者努力佈下天羅地網，希望逮到愈多受害者愈好。有了目標式勒索軟體，攻擊者採用更實用的方法，將心力投注於特定目標。

例如，SamSam 鎖定執行未修補 Red Hat JBoss (又稱為 WildFly) 的伺服器，而非透過垃圾郵件或偷渡式下載攻擊鎖定個人使用者。SamSam 攻擊者利用可免費取得的工具 (例如，開放原始碼測試工具 JexBoss)，找出易受攻擊的伺服器。進入之後，攻擊者會在加密任何檔案之前，先竊取憑證，並進行進一步的偵查。威脅使用開放原始碼與大眾熟知的工具，可規避偵測雷達，因為許多工具 (例如 SamSam 使用的 Microsoft Sysinternals) 是常見的企業網路工具。

目標式勒索軟體攻擊的另一個例子是，Bucbi 勒索軟體背後的犯罪份子如何入侵 RDP 伺服器。進入網路之後，攻擊者會使用 RDP 伺服器進行橫向移動，並花一些時間偵查，了解企業的備份政策。攻擊者獲得所需的資訊後，便會啟動勒索軟體，將在電腦上或連接至 RDP 伺服器之其他伺服器上找到的檔案加密。他們不用傳統方式索取贖金，而是改用電子郵件，因此犯罪份子可利用偵查期間獲得的資訊，交涉更高的金額。

目標式攻擊與傳統勒索軟體間的另一個差異是，設定加密所使用的方法。一般情況下，勒索軟體會聯絡指令與控制 (C&C) 伺服器，然後伺服器會產生 RSA 金鑰配對，並將公開金鑰傳回惡意程式，在加密階段使用。不過，SamSam 攻擊者則是在感染鎖定的伺服器時，產生自己的 RSA 金鑰配對，並透過勒索軟體上傳公開金鑰。

也有入侵伺服器的勒索軟體，在等待了好幾個月之後才要求付款。PHP.Ransomcrypt.A 威脅會默默地將寫入受感染網頁伺服器的資料加密，然後在資料被讀取時解密。等待足夠的時間後，攻擊者會將私密加密金鑰從伺服器中移除，並將勒索信傳送給網站負責人。這段等待期間是為了確保在勒索贖金之前，將所有增量備份加密。

主要鎖定企業的攻擊者必須先在網路上獲得立足點，才能散播勒索軟體。如同先前所述，伺服器是一個理想的攻擊目標，可透過以下方法來鎖定：

- 用於 RDP 伺服器的強制破解憑證，例如 Bucbi
- 鎖定網頁外掛程式中的漏洞，取得網頁伺服器的存取權限，例如 Linux.Encoder
- 攻擊 JBoss 伺服器中的瑕疵，例如 SamSam

一旦伺服器遭入侵，攻擊者即可在網路內橫向移動，感染連線的電腦。

可區別目標式勒索軟體攻擊與傳統勒索軟體活動的一些要點包括：

- 使用先進的技術滲透到網路，例如攻擊漏洞
- 在網路間橫向移動，進而感染許多電腦或尋找有價值的目標，例如資料庫，以擴增攻擊的影響。這也讓攻擊者有充足的機會可以偵查目標。
- 利用合法工具，維持低調
- 刪除備份檔案，防止受害者復原受感染資料，促使他們支付贖金

消費者勒索軟體活動是自動化的，但是目標式攻擊的攻擊者本身需要進行很多工作。不過，可能的高獲利彌補了這項缺點，因為相較於消費者，企業可能擁有更高價值的重要資料資產與更深的口袋。

案例研究：作為誘餌的勒索軟體

賽門鐵克資安事端應變中心最近協助調查某家大型公司中疑似大規模的勒索軟體感染事件。表面上看起來似乎是公司中有上百台電腦遭受 CryptoWall 變種的感染。

偽裝的勒索軟體

賽門鐵克採集攻擊者使用的惡意程式和工具樣本之後，便開始進行分析。開始調查後不久便發現到，「勒索軟體」攻擊的背後一些耐人尋味的現象。當我們的調查人員檢查勒索軟體樣本時發現，該惡意程式並未實際加密任何檔案，而只是利用垃圾資料覆寫這些檔案。

名為 Trojan.Phonywall 的惡意程式，顯示的勒索信與實際的 CryptoWall 訊息相同，唯一的差異在於付款網址。每次感染通常都會附帶專屬的 CryptoWall 付款網址，但是 Phonywall 的付款網址則經過硬式編碼，並且是從已在網路上發佈的 CryptoWall 勒索信複製過來而已。

APT 攻擊的相似點

精心設計的目標式攻擊利用偽裝的勒索軟體，讓人無法注意到攻擊者的真正目的 (竊取資料)，然而揭發這些攻擊的第一步就是尋找誘餌。

這類攻擊與 APT 攻擊有許多相似之處。賽門鐵克發現，在部署誘餌勒索軟體之前，攻擊者早已入侵公司長達五個月。為了在第一階段攻擊期間就找到入侵入口，網路罪犯會同時利用水坑式攻擊與夾帶惡意附件的魚叉式網路釣魚電子郵件。接著，攻擊者使用後門惡意程式與免費取得的滲透測試工具，穩固他們在網路中的地位，繼續入侵系統管理員帳戶憑證。然後他們會使用這個系統管理員帳戶憑證入侵公司內部檔案、應用程式與電子郵件伺服器，以及多台工作站。

隱匿其蹤跡

經過大約五個月之後，攻擊者設法先從鎖定的公司竊取數以千計的檔案，然後再嘗試利用 Phonywall 誘餌隱匿其蹤跡。攻擊者使用竊取得來的系統管理員憑證，將 Phonywall 部署至公司中 33% 的工作站。偽裝的勒索軟體威脅總共覆寫了 723 台電腦上的資料。

過去曾有攻擊者部署 DDoS 攻擊來掩蓋入侵行為。不過，使用類似勒索軟體的活動作為誘餌，是另一個引人關注的攻擊掩飾手法。

學到的教訓

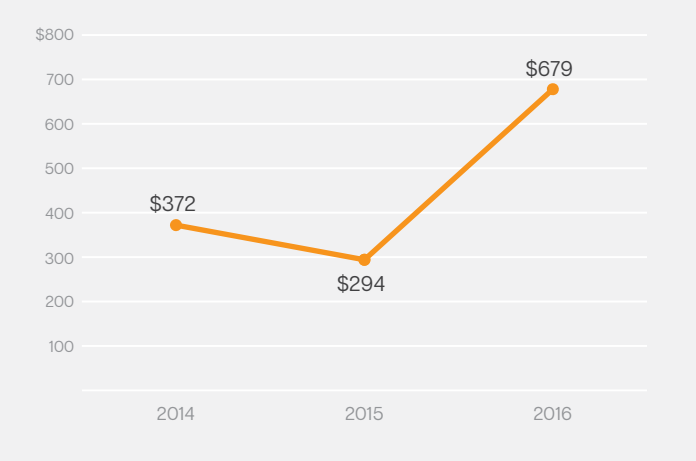
1. 勒索軟體已成為司空見慣的威脅態勢。認為已遭受勒索軟體感染的企業可能會決定接受現況，不做任何進一步的調查。同時，表面的勒索軟體攻擊可能只是一種干擾手法，真正的惡意行為是竊取資料。
2. 網路罪犯現在已瞭解大多數人已大略認識勒索軟體，以及勒索軟體所帶來的威脅。攻擊者可能會利用人們對勒索軟體的瞭解，隱匿更多進階攻擊。
3. 攻擊者會在第一階段攻擊使用魚叉式網路釣魚電子郵件。員工訓練可降低員工第一時間開啟惡意電子郵件的風險。
4. 與賽門鐵克資安事端應變中心合作，客戶可揭發攻擊者的真正目標，處理公司資料遭竊問題，而不是支付贖金之後，卻仍無法復原任何檔案。

勒索軟體的影響

攻擊者要求的平均贖金在今年又再次攀升。2016 年迄今為止發現的平均贖金已從 2015 年的 294 美元增加到 679 美元。贖金要求的逐漸增加表示攻擊者可能認為可以從受害者壓榨更多金錢。

今年，攻擊者要求的贖金也創下新高，名為 7ev3n-HONE$T (Trojan.Cryptolocker.AD) 的威脅就要求每台電腦支付 13 枚比特幣的贖金 (在 2016 年 1 月發現該威脅當時，相當於 5,083 美元)。這是賽門鐵克至今看過最高的金額。

圖 13. 每年平均贖金金額 (以美元計)



損失的規模

並無法準確地計算勒索軟體受害者支付給攻擊者的金額。少有受害者會透露他們是否已支付贖金。攻擊者鮮少透露他們賺了多少錢，且每個感染一般都有專屬的加密貨幣錢包，因此難以追蹤款項。在攻擊者兌現之前，會透過各個不同錢包和「洗錢」服務經常流動贖金。

然而，部分執法機關公佈的統計數字，足以洞察損失的規模。FBI 反映在 2015 年收到 2,400 件關於勒索軟體的投訴，據報損失超過 2,400 萬美元。此數字超過 2014 年備案的 1,800 件以上投訴，據報損失 2,300 萬美元。

光從美國的預估數字來看，可合理地推斷主要勒索軟體變種背後的攻擊者每年應可賺取上千萬美元。此外，可能因為沒有別的選擇，因此絕大多數的受害者似乎願意支付贖金。

從美國 IDT911 最近一項針對中小型企業所做的研究顯示，84% 的人表明受到攻擊時，不會支付贖金。另一份德國的報告顯示，參與調查的企業中，有 32% 在過去六個月內發生勒索軟體事件。在這些企業中，有 95% 表示他們未支付贖金給攻擊者。

攻擊的實際成本

在 2016 年 2 月初，美國好萊塢長老教會醫療中心 (HPMC) 遭到勒索軟體入侵。醫院承認支付攻擊者要求的 17,000 美元來還原系統，其中部分系統可存取病患醫療紀錄。然而，當企業發生此類事件，17,000 美元可能只佔潛在成本 (金錢和聲譽) 的一小部分。

企業受到勒索軟體攻擊之後，可能面臨的潛在影響如下：

- **停機時間成本**：企業可能被迫關閉系統來處理感染事件。鎖定的企業服務遭受影響，進而連帶波及消費者。企業可能因為停機而造成財務損失及名譽受損。如果是公用事業公司，停水或停電可能會影響上百萬人，並因意外事故導致受傷，甚至造成死亡。
- **財務成本**：公司為了應付勒索軟體，可能必須支付資安事端應變和其他安全相關解決方案的費用。若客戶受到影響，企業可能也需支付龐大的法律費用。可能需支付罰金或罰緩。例如，違反健康保險流通與責任法案 (HIPAA) 的美國醫院需支付高達 100 萬美元的罰金。
- **資料外洩**：由於文件遭到加密及/或遭竊而造成資料外洩，會對企業造成嚴重的影響。公司記錄、客戶個人識別資訊 (PII) 或智慧財產權的外洩，將嚴重影響企業的財務、品牌與商譽。主導攻擊的網路罪犯可能會威脅將竊取的資料公諸於網路，試圖從受害者身上勒索更多金錢 (我們已發現 Chimera 的作者使用此手法)。就算受害者支付贖金，網路罪犯將檔案解密，在解密的過程中，資料仍可能受到損壞。
- **人命損失**：當醫院或其他醫療機構遭受感染，受到影響的重要醫療設備則可能會危害病患的生命。可能無法存取內含病史的病歷資料，導致治療延遲或甚至施用不正確的藥物。

勒索軟體攻擊會影響企業永續性、生產力、公司財務、名譽，甚至是企業的安全。雖然攻擊一開始的衝擊可能很大，但長期影響的代價可能更為昂貴。■

防護

採用多層式安全方法，將感染的機會降至最低。賽門鐵克利用三階段策略，抵禦勒索軟體：

1. 防護
2. 抑制
3. 應變

1. 防護

避免感染是最具成效的作法，因此留意防止感染的作法是值得的。電子郵件與刺探套件是勒索軟體最常見的感染媒介。針對這兩種感染媒介採取強大的防禦機制，有助於降低感染的風險。

電子郵件安全

如 Symantec Email Security.cloud 這類電子郵件過濾服務，可阻絕惡意電子郵件接觸使用者。Symantec Messaging Gateway 的 Disarm 技術可將附加文件的惡意內容移除，保護電腦不受威脅。

電子郵件雲端服務技術擁有即時連結追蹤 (Real Time Link Following，簡稱 RTLF) 功能，可處理附件中的網址，而不只是電子郵件內文。之外，電子郵件雲端服務擁有的先進功能，可透過程式碼分析與模擬，偵測並攔截電子郵件中的惡意 JavaScript。

入侵預防

賽門鐵克入侵預防系統 (Intrusion Prevention System，簡稱 IPS) 技術可偵測並攔截來自刺探套件活動的惡意流量，阻止安裝勒索軟體。

Download Insight

賽門鐵克 Download Insight 技術可檢查透過 Web 瀏覽器、即時通訊用戶端及其他入口網站下載或啟動的檔案。Download Insight 能根據信譽，判斷檔案是否具有風險。

瀏覽器防護

賽門鐵克的瀏覽器防護解決方案可分析 Web 瀏覽器的狀態，阻止網站傳送攻擊。

入侵防護

賽門鐵克的入侵防護技術，可識別許多在入侵攻擊中常見的惡意行為，並將其封鎖使攻擊無法執行。

最佳實務準則

建議一般使用者立即刪除收到的所有可疑電子郵件，特別是包含連結及/或附件的電子郵件。

務必留意提示使用者啟用巨集的 Microsoft Office 附件。雖然巨集有自動化作業等合法用途，但攻擊者常利用惡意巨集，透過 Office 文件傳送惡意程式。為了消弭這個感染媒介，Microsoft 已預設停用從 Office 文件中載入的巨集。攻擊者可能會利用社交工程技術，說服使用者啟用巨集。因此，賽門鐵克建議使用者避免在 Microsoft Office 中啟用巨集。

2. 抑制

一旦受到感染，關鍵步驟是抑制攻擊的蔓延。賽門鐵克的檔案型技術能確保電腦下載的所有酬載無法執行常式。

賽門鐵克擁有 24 小時全年無休的賽門鐵克安全機制應變中心 (STAR) 團隊，負責持續開發、改善針對勒索軟體的一般特徵。團隊會持續監控勒索軟體及其傳送鏈，以收集新樣本，確保偵測功能固若金湯。

先進的防毒引擎

賽門鐵克使用偵測引擎陣列，包括利用啟發式技術的特徵式進階防毒引擎、即時 (JIT) 記憶體掃描、機器學習引擎，以及 Malheur。

防護

SONAR 行為引擎

SONAR 是賽門鐵克即時行為型防護，可防止潛在的惡意應用程式在電腦上執行。不需任何特定的偵測特徵，即可偵測惡意程式。SONAR 使用啟發式、信譽資料與行為策略，偵測新興和未知的威脅。SONAR 可偵測勒索軟體常見的加密行為。

機器學習技術

賽門鐵克的改良式機器學習探索技術，已專門針對勒索軟體進行訓練。這項強大的技術無須另外要求程式碼，即可識別新的勒索軟體。

模擬器

模擬器不需使用特徵，即可讓引擎以啟發的方式偵測加密行為。

最佳實務準則

執行完整的網路掃描，找出所有受感染的電腦。將遭入侵的電腦從網路中隔離，直到電腦清理完畢並還原。

3. 應變

企業可採用幾個步驟，確保早日從勒索軟體感染中復原。

資安事端應變

賽門鐵克資安事端應變 (IR) 可協助企業應變攻擊，並決定下一步該怎麼做。

協助找出主要的感染程式並遏制進一步擴散：找出主要的攻擊才能了解攻擊者主要活動鎖定的目標，確保您不會因為只專注在勒索軟體上，而錯過實際的攻擊。

針對資安事端提出專屬建議，防止日後發生類似攻擊：我們可以幫助客戶實施控管，避免任何進一步的疫情，並協助他們加強端點防護環境。在過去發生的資安事端中，我們僅僅花了 72 小時，就能大幅增強反覆受勒索軟體攻擊的受害者企業安全環境。

我們分析惡意程式，判斷資料的加密方式，協助受害者建立資料復原計劃：在許多情況下，惡意程式撰寫者所犯下的執行錯誤，讓資安事端應變人員得以輕鬆地復原資料。技術純熟的惡意程式分析師可針對勒索軟體進行反向工程，找出當中執行的弱點，幫助使用者復原資料。

依照不同威脅，與客戶的資料復原供應商合作，決定最佳計劃：客戶常會租用資料復原服務，來協助進行勒索軟體復原程序。復原過程因人而異，而且主要取決於所使用的惡意程式複雜性。分析惡意程式、了解加密方式及清除資料之後，賽門鐵克資安事端應變可與資料復原供應商合作開發有效的資料復原計劃。

最佳實務準則

備份重要資料是打擊勒索軟體感染的其中一個重要基石。然而，過去曾發生勒索軟體加密備份的情況，因此備份不能取代穩固的安全策略。

受害者必須明白，支付贖金不是一勞永逸的辦法。攻擊者有可能不送出解密金鑰、解密程序執行方式不佳而損害檔案，也可能在收到頭期款後，再要求更高的贖金。■

附錄：
賽門鐵克偵測到的常見勒索軟體

下列是最近常見的勒索軟體名稱清單，以及賽門鐵克對這些軟體的偵測名稱。贖金要求以美元計價反映出勒索軟體發佈當時的貨幣價值：

表格：常見的勒索軟體偵測名稱、發現月份，以及贖金價格

發現時間	類型	常見名稱/別名	要求的贖金	賽門鐵克偵測的名稱
2016 年 5 月	加密型	Mischa	大約2 枚比特幣	Trojan.Cryptolocker.AP
2016 年 5 月	加密型	Alpha Locker	400 美元的 iTunes 點數	Trojan.Ransomcrypt.AM
2016 年 5 月	加密型	MM Locker	大約400 美元的比特幣	Trojan.Ransomcrypt.AN
2016 年 5 月	加密型	Bucbi	5 枚比特幣	Trojan.Ransomcrypt.AO
2016 年 5 月	加密型	Enigma	0.42 枚比特幣	Trojan.Ransomcrypt.AP
2016 年 5 月	加密型	Mobef/Yakes	4 枚比特幣	Trojan.Ransomcrypt.AQ
2016 年 5 月	加密型	Shujin	未知	Trojan.Ransomcrypt.AR
2016 年 5 月	加密型	CryptoHitman	150 美元的比特幣	Trojan.Ransomcrypt.AS
2016 年 4 月	加密型	Nemucod 7-Zip	0.52985 枚比特幣	JS.Ransomcrypt
2016 年 4 月	加密型	KimcilWare	1 枚比特幣	PHP.Ransomcrypt.B
2016 年 4 月	加密型	Rokku	0.24 枚比特幣	Trojan.Cryptolocker.AK
2016 年 4 月	加密型	Zeta/CryptoMix	未知	Trojan.Cryptolocker.AL
2016 年 4 月	加密型	Kovter	未知	Trojan.Cryptolocker.AM
2016 年 4 月	加密型	CryptXXX	500 美元的比特幣	Trojan.Cryptolocker.AN
2016 年 4 月	加密型	Yougothacked	0.5 至 1.5 枚比特幣	Trojan.Cryptolocker.AO
2016 年 4 月	加密型	Sanction/Rush	3 枚比特幣	Trojan.Ransomcrypt.AH
2016 年 4 月	加密型	CryptoHost/Manamecrypt/ROI Locker	0.3 枚比特幣	Trojan.Ransomcrypt.AI
2016 年 4 月	加密型	Jigsaw	0.4 枚比特幣	Trojan.Ransomcrypt.AJ
2016 年 4 月	加密型	AutoLocky	0.75 枚比特幣	Trojan.Ransomcrypt.AK
2016 年 4 月	加密型	TrueCrypter	0.2 枚比特幣	Trojan.Ransomcrypt.AL
2016 年 4 月	鎖定型	BrLock	未知	Trojan.Ransomcrypt.AQ
2016 年 4 月	鎖定型	Rasith	4 美元	W32.Ransomlock.AP
2016 年 3 月	鎖定型	AndroidOS_Locker	10,000 日圓	Android.Lockdroid.H
2016 年 3 月	加密型	KeRanger	1 枚比特幣	OSX.Keranger
2016 年 3 月	加密型	PHP CTB-Locker	0.4 至 0.8 枚比特幣	PHP.Cryptolocker.G
2016 年 3 月	加密型	Cerber	1.24 至 2.48 枚比特幣	Trojan.Cryptolocker.AH
2016 年 3 月	加密型	Maktub	1.4 至 3.9 枚比特幣	Trojan.Cryptolocker.AI
2016 年 3 月	加密型	Petya	0.99 枚比特幣	Trojan.Cryptolocker.AJ

發現時間	類型	常見名稱/別名	要求的贖金	賽門鐵克偵測的名稱
2016 年 3 月	加密型	Samas/SamSam	1.5 枚比特幣	Trojan.Ransomcrypt.AE
2016 年 3 月	加密型	Coverton	1 枚比特幣	Trojan.Ransomcrypt.AF
2016 年 3 月	加密型	Cryptohasyou	300 美元	Trojan.Ransomcrypt.AG
2016 年 3 月	鎖定型	Homeland Security Screen Locker	500 美元	Trojan.Ransomcrypt.AN
2016 年 2 月	加密型	HydraCrypt/UmbreCrypt	0.5 至 1.5 枚比特幣	Trojan.Cryptolocker.AE
2016 年 2 月	加密型	Locky	0.5 至 1 枚比特幣	Trojan.Cryptolocker.AF
2016 年 2 月	加密型	PadCrypt	0.8 枚比特幣	Trojan.Cryptolocker.AG
2016 年 2 月	加密型	Job Crypter	300 歐元	Trojan.Ransomcrypt.AC
2016 年 2 月	加密型	RackCrypt/MVP Locker	1.3 枚比特幣	Trojan.Ransomcrypt.AD
2016 年 1 月	加密型	CryptoJoker	未知	Trojan.Cryptolocker.AC
2016 年 1 月	加密型	7ev3n/HONE$T	13 枚比特幣	Trojan.Cryptolocker.AD
2016 年 1 月	加密型	DMA-Locker	1.5 至 15 枚比特幣	Trojan.Ransomcrypt.AA
2016 年 1 月	加密型	LeChiffre	未知	Trojan.Ransomcrypt.AB
2016 年 1 月	加密型	Ransom32	0.1 枚比特幣	Trojan.Ransomcrypt.Y
2016 年 1 月	加密型	NanoLocker	0.1 至 1 枚比特幣	Trojan.Ransomcrypt.Z
2015 年 12 月	加密型	Radamant	0.5 枚比特幣	Trojan.Ransomcrypt.W
2015 年 12 月	加密型	Hi Buddy!	0.3 至 0.7 枚比特幣	Trojan.Ransomcrypt.X
2015 年 11 月	加密型	Mabouia	無	OSX.Ransomcrypt
2015 年 11 月	加密型	CryptoWall 4.0	1.56 枚比特幣	Trojan.Cryptodefense.B
2015 年 11 月	加密型	CryptInfinite/DecryptorMax	500 美元	Trojan.Cryptolocker.AB
2015 年 11 月	加密型	Linux.Encoder.1	未知	Unix.Ransomcrypt
2015 年 11 月	加密型	Linux.Encoder.2	1 枚比特幣	Unix.Ransomcrypt.B
2015 年 10 月	鎖定型	RansomFake	未知	JS.FakeRansom
2015 年 10 月	加密型	Chimera	0.93 至 2.45 枚比特幣	Trojan.Ransomcrypt.V
2015 年 9 月	加密型	CryakI/Vipasana	未知	Trojan.Ransomcrypt.U
2015 年 8 月	加密型	ORX-Locker	0.525 枚比特幣	Trojan.Cryptolocker.AA
2015 年 8 月	加密型	Safefiles32	未知	Trojan.Cryptolocker.X
2015 年 8 月	加密型	Hidden Tear/EDA2/Magic/Surprise	未知	Trojan.Cryptolocker.Y
2015 年 8 月	加密型	CryptoApp	1 枚比特幣	Trojan.Cryptolocker.Z
2015 年 8 月	鎖定型	Department of Justice (DOJ) 新變種	未知	W32.Ransomlock.AQ!inf
2015 年7 月	加密型	Encryptor RaaS	0.174 枚比特幣	Trojan.Cryptolocker.W
2015 年 6 月	加密型	Troldesh/Shade	1 枚比特幣	Trojan.Ransomcrypt.T
2015 年 5 月	加密型	Breaking Bad/El-Polocker	450 美元至 1000 美元	Trojan.Cryptolocker.S
2015 年 5 月	加密型	Pollcrypto	1 至 2 枚比特幣	Trojan.Cryptolocker.T
2015 年 5 月	加密型	Tox	隨機	Trojan.Cryptolocker.U

發現時間	類型	常見名稱/別名	要求的贖金	賽門鐵克偵測的名稱
2015 年 5 月	加密型	鎖定型	0.1 枚比特幣	Trojan.Cryptolocker.V
2015 年 4 月	加密型	PClock2	0.5 枚比特幣	Trojan.Cryptolocker.Q
2015 年 4 月	加密型	Kriptovor	未知	Trojan.Cryptolocker.R
2015 年 4 月	加密型	Threat Finder	1.2 枚比特幣	Trojan.Ransomcrypt.S
2015 年 3 月	加密型	CryptoFortress	1 枚比特幣	Trojan.Cryptolocker.H
2015 年 3 月	加密型	Pacman	未知	Trojan.Cryptolocker.P
2015 年 3 月	加密型	BandarChor	未知	Trojan.Ransomcrypt.Q
2015 年 3 月	加密型	VaultCrypt/XRTN	未知	Trojan.Ransomcrypt.R
2015 年 2 月	加密型	TeslaCrypt	2 枚比特幣	Trojan.Cryptolocker.N
2015 年 1 月	加密型	Ransomweb	未知	PHP.Ransomcrypt.A
2015 年 1 月	加密型	CryptoTorLocker2015	100 美元的比特幣	Trojan.Cryptolocker.M
2015 年 1 月	加密型	Pclock	1 枚比特幣	Trojan.Ransomcrypt.P

參與人員

Dick O'Brien，編輯
John-Paul Power，助理編輯
Scott Wallace，平面設計

執筆人

Asim Rab
Alan Neville
Ayush Anand
Candid Wueest
Dennis Tan
Hon Lau
Jon DiMaggio
Joseph Graziano
Laura O'Brien
Orla Cox
Peter Coogan
Steve Meckl
Yek Loong Chong

特別感謝

Jennifer Duffourg
Mara Mort
Matt Nagel
Steve Meckl
William Wright

變更記錄

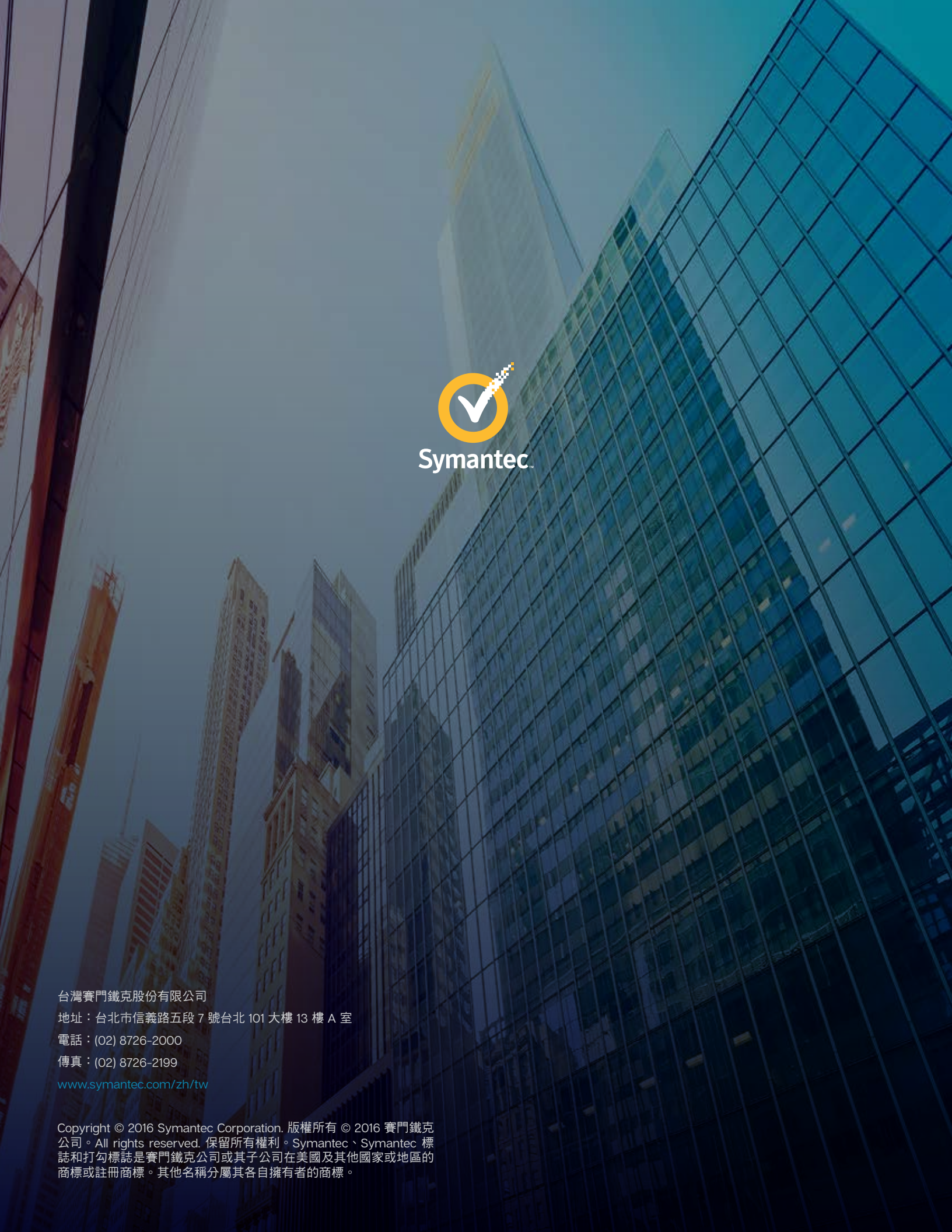
- 2016 年 8 月 10 日：更正地區和感染資料。
- 2016 年 7 月 19 日：首次出版。

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC) 是網路安全領域的全球領導廠商。我們運行全球規模最大的網路情報網之一，因而得以發現更多線上威脅，並保護更多客戶免於遭受新一代網路攻擊。無論最重要的資料存放於何處，我們都能協助公司、政府機構和個人妥善保存。

更多資訊

- 全球賽門鐵克：http://www.symantec.com/
- ISTR 與賽門鐵克情報資源：http://www.symantec.com/threatreport/
- 賽門鐵克安全機制應變中心：http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/



台灣賽門鐵克股份有限公司
地址：台北市信義路五段 7 號台北 101 大樓 13 樓 A 室
電話：(02) 8726-2000
傳真：(02) 8726-2199
www.symantec.com/zh/tw