Symantec by Broadcom

防禦勒索軟體

Symantec® Email Security.cloud (ESS)

賽門鐵克郵件安全雲端服務

如何阻止並防禦勒索軟體對電子郵件攻擊

產品型錄

挑戰

網路犯罪分子不斷改進他們的勒索軟體策略，利用網路釣魚、零時差攻擊和被入侵的帳戶來繞過傳統的安全防禦機制。

機會

部署賽門鐵克郵件安全雲端服務 (Symantec Email Security.cloud Service--以下簡稱 ESS) 的多層次電子郵件安全解決方案，可協助組織主動偵測勒索軟體威脅，並在威脅傳送至使用者之前加以阻擋。

效益

ESS 提供進階的威脅偵測、即時連結分析和行為監控，強化電子郵件安全性；降低勒索軟體感染的風險，並將成本高昂的業務中斷降到最低。

概觀

勒索軟體仍是組織最嚴重的網路威脅之一，而電子郵件則是主要的攻擊媒介。根據《2024 年 Verizon 資料外洩調查報告》，電子郵件是散播勒索軟體的主要管道，也是常見的第二大資料外洩媒介。勒索軟體會加密檔案或將使用者反鎖於系統之外，並要求使用者付款以恢復系統或資料的存取。根據 Chain Analysis 的報告，2023 年勒索軟體的支付金額超過 10 億美元，突顯這類攻擊所造成的財務損失。Verizon 報告也發現，近三分之一的資料外洩事件與勒索軟體或敲詐策略有關，影響 92% 的產業。此外，《2024 年 IBM 資料外洩成本報告》指出，與勒索軟體相關的資料外洩事件在過去一年增加了 41%，而且辨識和控制所需的時間也大幅延長。儘管最近執法單位採取行動，包括逮捕 LockBit 勒索軟體集團的主要成員，但攻擊數量仍然沒有任何改變。勒索軟體的持續威脅突顯了強大網路安全防禦的必要性。

面對勒索軟體的挑戰

預防勒索軟體透過電子郵件來發動攻擊正面臨多項挑戰，但以下四項是最重大挑戰：

精確的社交工程攻擊策略

攻擊者使用非常具有說服力的網路釣魚電子郵件，誘騙使用者開啟惡意附件或點選有害鏈結。這些電子郵件通常會冒充可信賴的聯絡人、要求採取緊急措施的業務要求，或利用心理操控來繞過使用者的懷疑。即使是訓練有素的員工也可能成為這些不斷翻新的攻擊伎倆的受害者，使得人為錯誤成為持續的挑戰。

惡意軟體和零時差威脅

網路犯罪份子不斷開發新的勒索軟體，以躲避傳統的安全防護機制。許多攻擊開採濫用零時差漏洞或使用多形態的惡意軟體，這些惡意軟體會變更程式碼，以避免被特徵碼比對式的安全解決方案偵測到。如果沒有進階的威脅偵測技術，組織很難在系統被滲透前識別並阻止這些不斷進化的威脅。

濫用遭到入侵帳戶的危害愈來愈嚴重

攻擊者通常會透過竊取憑證或憑證網路釣魚擄獲合法的電子郵件帳戶，讓他們可以從可信的來源散佈勒索軟體。由於這些電子郵件來自已知的連絡人，因此可以輕易繞過安全濾網，並降低收件者的懷疑。偵測遭到入侵的帳戶需要進階的行為分析和即時監控，以便在損害發生之前識別異常活動。

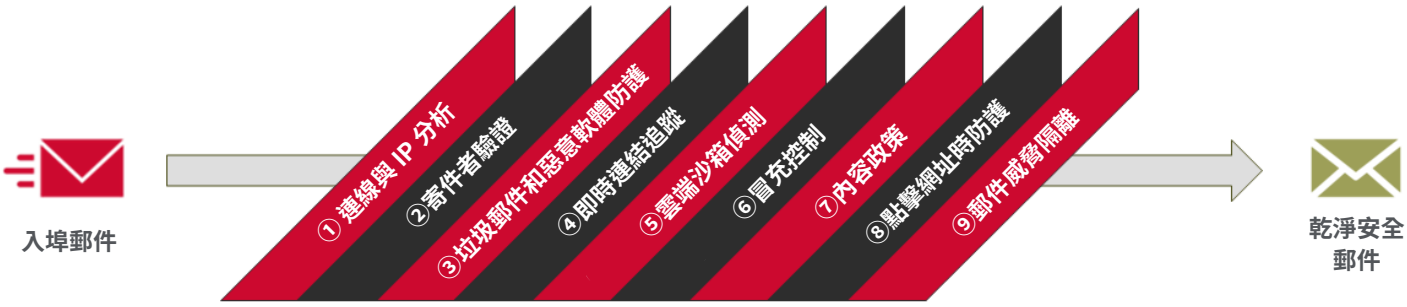
採用混淆技術讓攻擊鏈變得更複雜以規避傳統電子郵件安全解決方案的偵測

惡意軟體不再以電子郵件附件的方式傳送，而是以網頁下載的方式傳送。這些下載通常會混淆在縝密複雜的攻擊鏈的末端，其中可能包括多個網頁重新導向、合法的文件共享網站和不同的檔案下載。為了應付這些挑戰，組織需要強韌的多層次電子郵件安全策略，包括進階的威脅偵測、落實使用者訓練和主動監控，以保持防護技術能領先於攻擊者。本文將探討賽門鐵克郵件安全雲端服務 (Symantec Email Security.cloud Service--簡稱 ESS) 如何提供這些必要的防護，以協助組織預防勒索軟體透過電子郵件來發動攻擊。

賽門鐵克的解決方案

賽門鐵克 ESS 是進階的智慧型電子郵件安全平台，專為加強電子郵件系統的原生安全性而生，同時將誤報率降至最低。賽門鐵克 ESS 採用尖端技術，包括即時連結分析、雲端沙箱、點擊時保護和郵件安全隔離；所有這些技術都由賽門鐵克全球情報網路的遙測技術所提供。這些功能可讓 Symantec ESS 攔截複雜的電子郵件威脅，例如：勒索軟體、魚叉式網路釣魚和商業電子郵件詐騙 (BEC)。

圖 1：賽門鐵克 ESS 提供的多層防禦



如圖 1 所示，賽門鐵克 ESS 提供多層防禦來保護您的電子郵件通訊。以下各節將更深入探討這些防禦措施。

①連線與網際網路通訊協定 (IP) 分析

賽門鐵克 ESS 提供的第一道防線是連線層級防護。許多電子郵件攻擊利用殭屍網路，其行為與合法的電子郵件伺服器不同。Symantec ESS 會即時評估 SMTP 連線，識別並丟棄那些源自非郵件伺服器的連線。同時，Symantec ESS 會檢查寄件者的 IP 位址，並針對任何列入黑名單的來源強制執行 DNS 封鎖。這兩層過濾層可防止約 44% 的惡意電子郵件流量 (根據賽門鐵克 ESS 的內部資料) 傳送至使用者。

②寄件者驗證

網路犯罪分子經常使用冒名手法，讓惡意電子郵件看似合法。為了對抗這種策略，賽門鐵克 ESS 會根據已公佈的驗證記錄 (SPF、DKIM、DMARC) 來驗證電子郵件是否來自授權系統或網域。如果電子郵件無法通過驗證，就會被定義為惡意而不會傳送至收件者。賽門鐵克 ESS 可偵測模仿受信任寄件者的偽造電子郵件，防止攻擊者誘騙員工開啟惡意電子郵件或分享敏感資訊。

③垃圾郵件和惡意軟體防護

賽門鐵克 ESS 利用信譽分析、防毒引擎和反垃圾郵件簽章來偵測和封鎖惡意附件和連結。傳統的簽章式偵測對已知的威脅非常有效，但現代的勒索軟體攻擊通常會使用武器化的網址連接 (URL) 而非附件來避開這些過濾機制。為了對抗這種策略，賽門鐵克 ESS 採用啟發式偵測，分析電子郵件模式和行為，在威脅造成危害之前先找出前所未見的威脅。

④即時連結追蹤 (Real-Time Link Following)

為了解決混淆下載的問題，賽門鐵克 ESS 最重要的防禦功能之一，即時連結追蹤 (Real-Time Link Following) 功能，會主動掃描和評估內送電子郵件中的內嵌網址連接 (URL)。即使攻擊者試圖透過重定向或短網址服務來混淆真正的網址連接 (URL)，賽門鐵克 ESS 仍會在電子郵件傳送之前，追蹤每個連結至其最終目的地。

例如：在 2024 年 4 月，一個名為 TA547 的垃圾郵件攻擊行動鎖定德國組織，透過以下攻擊鏈的手法傳送 Rhadamanthys 惡意竊密程式，之後再針對澳洲傳送金融類型勒索軟體有效酬載：

1. 向目標組織發送包含密碼保護的 .ZIP 附件的電子郵件。
2. 接收者在解壓縮 .ZIP 檔案時，會發現一個連結檔案。
3. 點擊該連結會下載 PowerShell 指令碼，該指令碼會傳送惡意軟體。

只有啟動所有步驟才能揭露此類型的攻擊，以確定最終結果。在這種情況下，賽門鐵克 ESS 會模擬使用者的動作，先解壓縮檔案、發現連結，然後追蹤連結以確定其最終導向。如果確定網址連接 (URL) 是惡意的，就會封鎖電子郵件。如果不確定，賽門鐵克 ESS 會根據各種因素指派風險評分、例如：網站註冊詳細資料和網路流量的類型。組織可以設定風險臨界值，以便在高風險電子郵件自動傳送給使用者之前將其攔截。透過在傳送前即時掃瞄連結，賽門鐵克 ESS 可協助瓦解依賴隱匿或新建立惡意網址連接 (URL) 的複雜勒索軟體活動。

⑤雲端沙箱偵測

賽門鐵克 ESS 包含雲端沙箱偵測，可偵測惡意指令碼和可執行檔。可疑的附件會在虛擬環境中執行，賽門鐵克 ESS 會在虛擬環境中監控其行為。賽門鐵克 ESS 會判斷附件是否構成威脅。雖然大多數的勒索軟體攻擊並不依賴傳統的可執行附件，但此功能可協助捕捉非傳統或新興的威脅。

⑥冒充控制

賽門鐵克 ESS 採用精密的防假冒寄件者引擎，可偵測並阻止模仿合法使用者、主管或可信網域的電子郵件。這種防護對於阻止勒索軟體和商業電子郵件詐騙 (BEC) 攻擊至關重要，因為這些攻擊經常會依賴假冒高階主管 (CxO) 詐騙和偽造供應商電子郵件來欺騙收件者下載惡意軟體或轉帳。透過識別試圖利用信任的欺詐電子郵件，賽門鐵克 ESS 可保護使用者避免被網路釣魚詐騙、避免成為勒索軟體的挾持受害者。

⑦內容政策

賽門鐵克 ESS 允許組織建立自訂郵件附加檔案封鎖規則，以防止接收或傳送高風險附件。如果組織不使用某些檔案類型 (例如：.exe、.scr 或啟用巨集的 Office 文件)，則可設定賽門鐵克 ESS，透過自動封鎖包含這些檔案類型的電子郵件來降低攻擊面。例如：組織可封鎖 JavaScript 和 VBScript 檔案，這些檔案通常用於以電子郵件為基礎的勒索軟體攻擊。客戶也可以針對電子郵件的其他方面建立客製化政策，包括網域的註冊時間，以及電子郵件正文和附件中所含網址連接 (URL) 的類別或風險等級。

⑧點擊網址時防護

攻擊者採用的另一種常見手法是在惡意連結發送後不久變更其目的地。這種伎倆可能會讓電子郵件繞過「掃描時」防護並傳送到收件者的收件匣。針對這些情況，「點擊時」防護可作為第二道防線。當使用者按一下連結時，賽門鐵克 ESS 會即時重新評估連結，跟蹤重定向並掃描目的地網址是否有威脅。如果連結最終指向已知的惡意網站，賽門鐵克 ESS 會立即攔截存取。如果網站可疑但未確認是惡意網站，連結會在「隔離環境」中開啟，以防止潛在傷害。由於網路犯罪分子經常在電子郵件傳送後更新惡意網址連接 (URL)，「點擊時」防護功能可確保即使是延遲的攻擊也能在執行前瓦解。此行為會自動套用至已知的惡意網址連接 (URL)，客戶也可依據超過 64 個預先建立的類別，建立自己的「點擊時」防護政策，以禁止不需要的網址連接 (URL)。

⑨郵件威脅隔離

賽門鐵克 ESS 採用電子郵件威脅隔離功能，可讓使用者遠離進階的網路釣魚和勒索軟體攻擊。如果使用者點選可疑連結，賽門鐵克 ESS 會遠端渲染網頁，防止惡意指令碼在使用者裝置上執行。此外，有潛在危險的下載也會在傳送前被掃描。透過隔離未知或高風險的網址連接 (URL)，賽門鐵克 ESS 可確保使用者無法與勒索軟體埋伏的網站直接互動，降低感染風險。

為什麼選擇 Symantec by Broadcom

勒索軟體仍然是最嚴重的網路威脅，而電子郵件則是其主要入侵點。賽門鐵克 ESS 結合即時連結分析、進階威脅偵測和行為監控，提供強大的多層次防禦功能，可在勒索軟體傳送至使用者之前加以阻止，以對抗這些不斷進化的攻擊。賽門鐵克 ESS 具備寄件者驗證、沙箱、冒充控制和點擊時防護等功能，可有效阻止網路釣魚嘗試、惡意附件和帳戶遭駭。將風險降到最低，並避免營運中斷的重大損失。隨著勒索軟體的策略日趨複雜，組織需要能夠因應新興威脅的主動式電子郵件安全，而賽門鐵克 ESS 可提供所需的情報與防護，讓組織持續地領先攻擊者。

如需詳細資訊，請造訪 www.broadcom.com/products/cybersecurity/email。

關於賽門鐵克

賽門鐵克公司 (Symantec) 已於 2019/11 合併入博通 (BroadCom) 的企業安全部門，Symantec 是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的政策性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。

若想瞭解更多資訊，請造訪原廠網站 https://www.broadcom.com/solutions/integrated-cyber-defense 或

賽門鐵克解決方案專家：保安資訊有限公司的中文網站 https://www.savetime.com.tw/(好記：幫您.節省時間.的公司.在台灣)

保安資訊 SAVETIME INFORMATION SECURITY

保安資訊有限公司｜地址：台中市南屯區三和街 150 號

電話：0800-381500｜+886 4 23815000｜www.savetime.com.tw