SOPHOS
Security made simple.

Intercept X + Sandstorm
加密勒索軟體最新解決方案

一、概述

根據 SOPHOS 威脅研究院的調查，目前無論是大、中還是小型企業都正受到越來越積極殘酷的加密勒索軟體攻擊所侵害。中招後用戶失去對重要檔案的存取權限，隨後被要求支付贖金，導致企業業務中斷。但你瞭解加密勒索軟體典型的攻擊方式嗎？什麼安全解決方案可以提供最好的防禦效果？本文研究了加密勒索軟體常用的進攻方式，看看為什麼攻擊能夠成功，並提供九個安全建議，以幫助你保持安全狀態。其中還說明了 IT 設置應包括的重大安全技術。

二、加密勒索軟體簡介

加密勒索軟體（Ransomware）是駭客用來劫持用戶資產或資源並以此為條件向用戶勒索錢財的一種惡意軟體。它是網際網路用戶面臨最廣泛和最具破壞性的威脅之一。自從惡名昭彰的 CryptoLocker 於 2013 年首次出現以來，我們見證到透過垃圾郵件和 Exploit Kits 所帶來了檔案加密勒索軟體演化的新時代，從家庭用戶和企業中敲詐金錢。

目前加密勒索軟體家族的演變可以透過“Locker”變種，將其根源追溯到早期的“假防毒”，最終到今天流行的檔案加密變種。每個不同類別的惡意軟體都有一個共同的目標 - 透過社交工程和威脅從受害者手中勒索金錢。每次反覆運算，對贖金的要求也變得更加龐大。

“加密勒索軟體”是近年數量增加最快的電腦網路威脅之一，駭客通常會隱藏蹤跡而要求使用者以電子貨幣方式支付贖金，以換取解密電腦資料所需的電子“金鑰”。 據估計，駭客借助此類軟體每年得手金額合計數億美元。據報導，好萊塢長老會醫療中心支付了 40 個比特幣（17,000 美元），以重新獲取其檔案，而堪薩斯心臟病醫院雖然支付了一筆未公佈的金額，但卻面臨著第二次贖金需求，而且沒有辦法存取其所有檔案。

三、為什麼加密勒索軟體會攻擊成功

大多數的企業都部署了某種形式的 IT 安全產品，為什麼勒索軟體還是能攻擊成功？

1. 先進的攻擊技術和不斷創新

1-1【駭客工具】讓想成為攻擊者中的一員越來越簡單，現今任何人都可以購買現成的 “勒索軟體即服務”（RaaS）工具來完成攻擊，得到並使用入侵程式變得越來越容易。攻擊者從而可以簡單地啟動，成功完成入侵，即使對於技術不足的攻擊者也可以輕易獲取利益。以下是一個 RaaS 程式銷售的案例。

包含感染網站的網路和端點技術，促使端點有效惡意掛載進而坐收推廣成效。

跨平台&能應對快速變化的軟體開發。

自動包含漏洞項目。

1-2【社交工程學】熟練的社交工程用於迷惑並提示使用者運行勒索軟體的安裝程式。例如，您可能會收到類似這樣標題的電子郵件：客戶需求在附件中，請提供我一個相關產品的報價。

1-3【專業性】加密勒索軟體的製造者以高度專業的方式運作。包括在支付贖金之後提供解密工具。

2. 安全性漏洞，作業系統和應用程式的更新Patch不能夠快速安裝

現在許多企業的 IT 管理員都已經認識到及時更新Patch的重要性，但是很難確保企業的這項政策能夠被員工迅速的執行和重視。

3. 安全系統配置不當

現今的資訊安全產品功能都十分多樣化，初衷是給用戶帶來 all in one 的解決方案，但很多產品配置起來過於繁瑣，很多管理員沒有很多時間去學習，無奈只能用到部分功能。如防毒軟體，防火牆，IPS，電子郵件/Web 閘道，未部署或未正確配置。

4. 缺乏先進的預防技術

勒索軟體的出現反應了傳統防毒的 “弱點”，勒索軟體會不斷更新，以及利用漏洞來避免被識別，甚至有自我保護機制。 例如，在將檔案加密後，對其自身進行快速刪除，使資安廠商無法對加密勒索軟體進行快速分析。

5. 缺乏安全知識與培訓

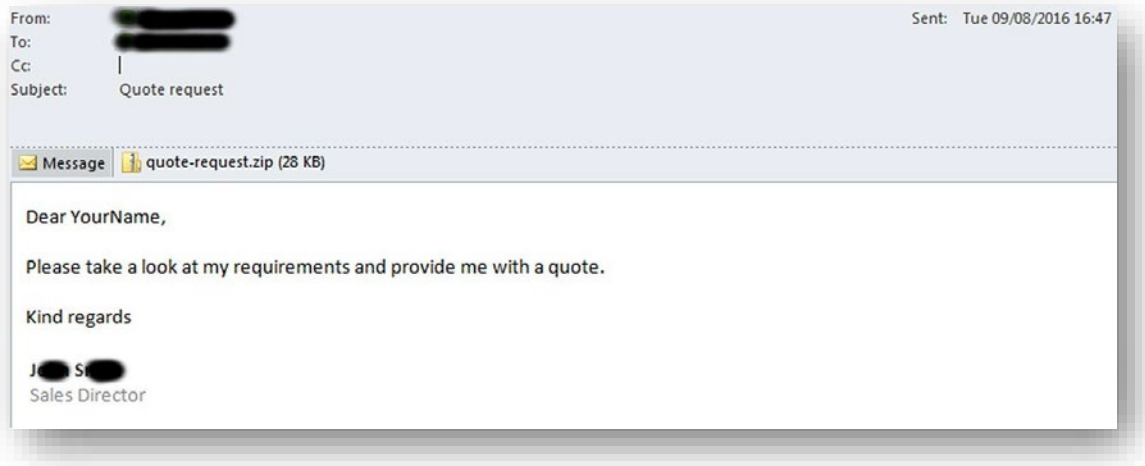
我可以打開哪些檔案並從哪些人獲取檔案？如果檔案看起來很可疑，該怎麼辦？如何識別網路釣魚電子郵件？

四、加密勒索軟體攻擊是如何展開的

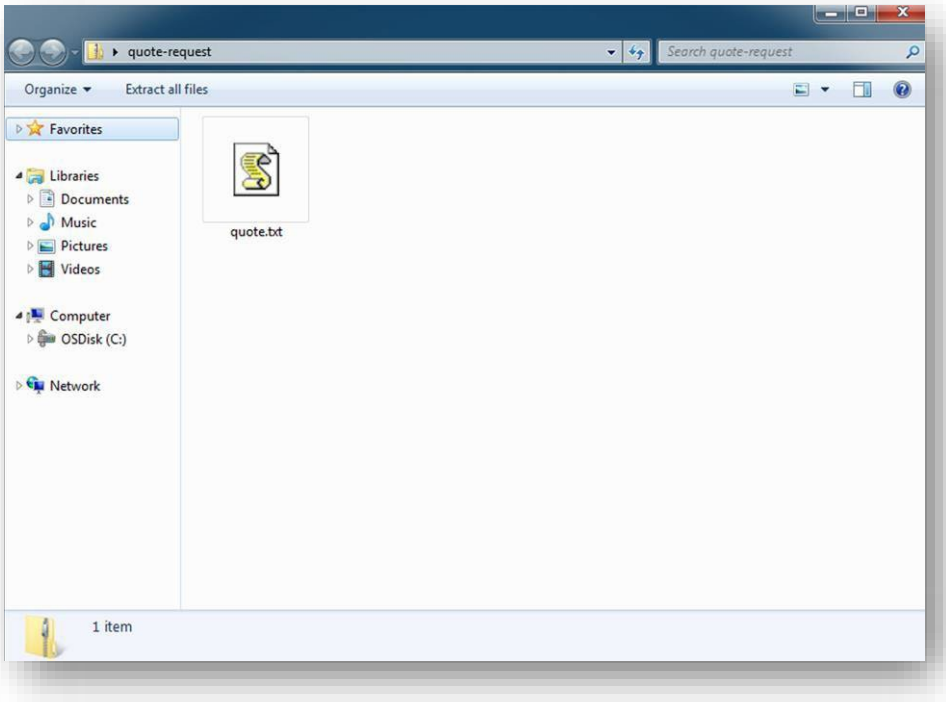
加密勒索軟體攻擊有兩種主要方式展開。透過帶有惡意附件的電子郵件，或透過存取被感染（通常是合法主流）的網站。

1. 惡意郵件

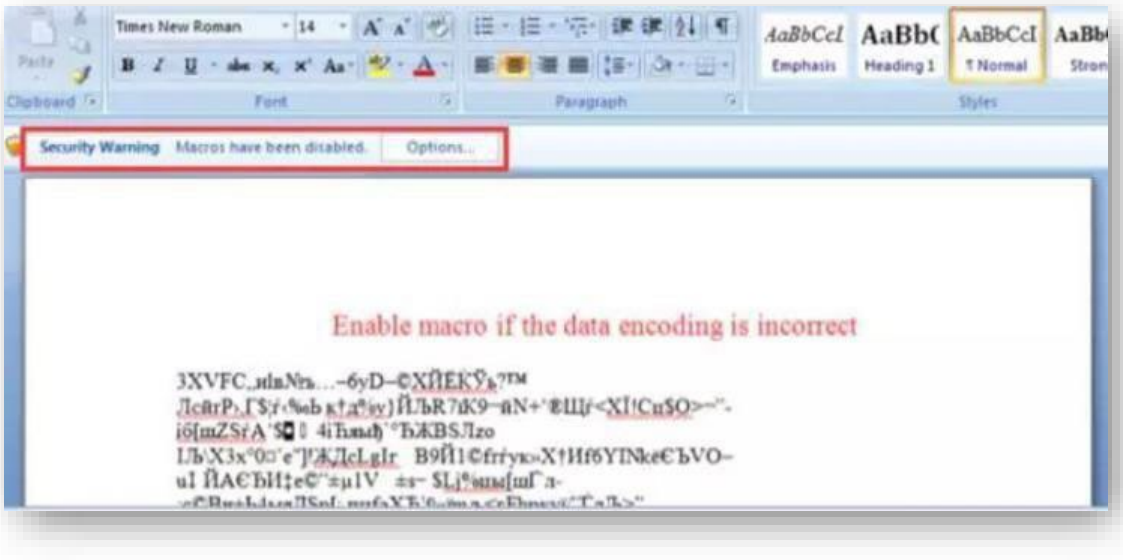
加密勒索軟體攻擊的一個主要途徑是透過郵件傳輸。今天的犯罪份子正在製作與正常無法區分的電子郵件。語法正確無拼寫錯誤，並且通常會編寫和您生活相關的內容。也就是，攻擊者會透過社交工程手段引誘受害者運行惡意郵件的附件。



附件的內容通常會偽裝成我們常見的格式，使我們卸下警戒心。



再以最近最知名的 Locky 勒索軟體攻擊原理為範例，勒索軟體一般會利用 Office 檔案巨集（現在的大部分文字處理程式，試算表和資料庫都包含功能強大的程式語言，允許在檔案中使用命令序列。這些命令序列或小程式就是所謂的巨集）的功能來執行惡意程式碼，例如打開一個 word 檔案，提示需要啟動巨集功能：



檔案打開後是亂碼，並有一行紅字標明如果無法正確解碼，請啟用巨集。如上圖中紅框所示，Word 檔案預設配置是停用巨集的。一旦使用者成功“被騙”啟用了巨集， 就會成功完成攻擊。

2. 惡意網站

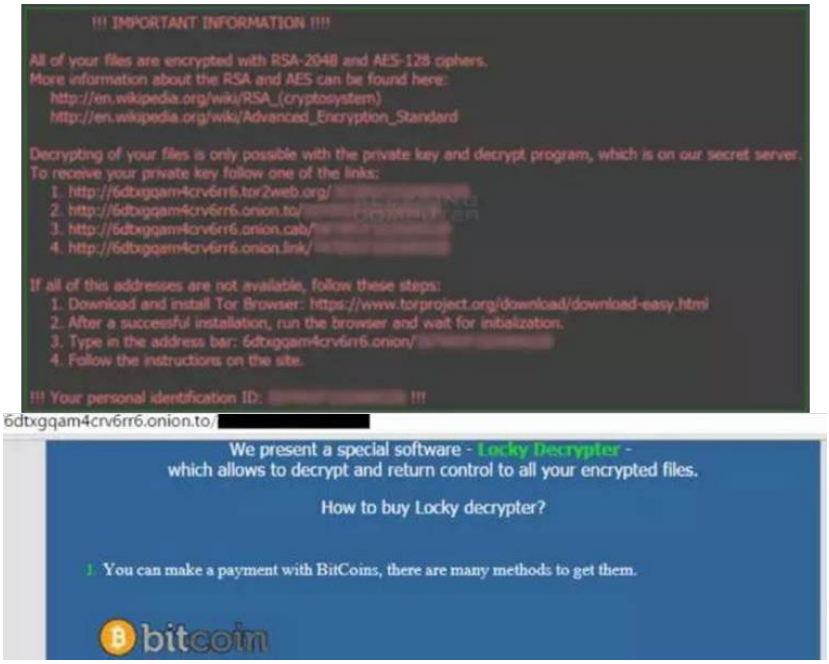
另一種常見的受到感染方法是存取了已被感染的合法網站。即使是主流網站也可能暫時被攻破。漏洞攻擊包是駭客用來利用已知或未知漏洞（例如零時差漏洞）的黑市工具。

您瀏覽到被駭客入侵的網站，然後點擊網站的連結廣告，或在許多情況下只查看網頁。這就足以下載加密勒索軟體檔案到您的電腦上運行，通常沒有可發現的跡象，直到攻擊完成。

五、加密勒索軟體攻擊成功

中招的結果就是可執行代碼會從遠端伺服器下載加密勒索軟體的本體到暫存資料夾，並自動執行，結果就是會在本地電腦，卸除式裝置和所有可存取的網路磁碟上加密特定檔案類型（根據勒索軟體類型而異），例如 Office 檔案、資料庫檔案、PDF、CAD 檔案、HTML、XML 等。而且會把檔案名稱混雜成不可閱讀的樣子並且更改副檔名（例如： F67091F1D24A922B1A7FC27E19A9D9BC.locky）。通常會刪除 Windows 作業系統的自動備份（陰影副本），以防止資料被恢復。

之後，在 Windows 桌面和每一個資料夾內都會出現一個新的txt 檔案，這個就是勒索資訊，同時桌面背景也會被勒索資訊所替換，要求受害者使用比特幣付款，通常勒索 1 個以上的比特幣（價值約 200 到 400 美金）。



勒索軟體攻擊過程如下：

六、SOPHOS 加密勒索軟體最新解決方案

針對加密勒索軟體的主要傳播途徑，以及變種快速，不易被特徵碼技術偵測的特點。

SOPHOS 最新推出了革新性的端點安全產品 — SOPHOS Intercept X。能在現有的端點安全（防毒）之上增添新世代防護技術，提供完整且多層式的保護。配合使用整合了Sandstorm（雲端沙箱技術）功能的SOPHOS 郵件安全閘道為使用者解決加密勒索軟體和釣魚郵件帶來的安全威脅。

1. SOPHOS Intercept X 簡介

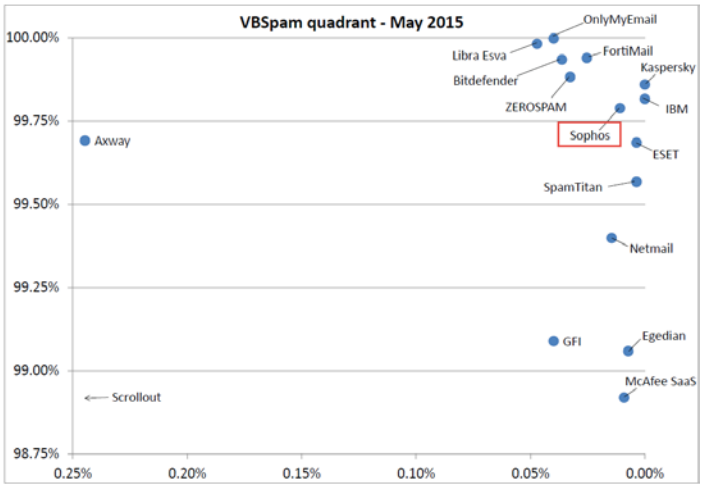
SOPHOS 新世代端點安全解決方案 Intercept X，主要目的在於阻止未知的威脅。有別於傳統的防毒軟體，SOPHOS Intercept X 不需要更新病毒定義資料庫，基於惡意行為分析阻止加密勒索行為。面對當今千變萬化的加密勒索軟體攻擊，Intercept X透過獨特的技術可以防止檔案被加密，並且能還原被加密的檔案。Intercept X 可以和原有SOPHOS 端點安全產品整合，也可以和其他防毒軟體相容使用。

2. SOPHOS Intercept X 的主要功能如下：

a) Cryptoguard：勒索軟體防護技術能偵測出自發性的惡意資料加密情形，阻斷加密勒索軟體的運作以及恢復被加密的軟體。
b) 入侵程式防禦：入侵程式防禦可辨識和阻擋常見的惡意攻擊工具滲透技術，在威脅形成問題前就加以阻擋，以便保護端點，防範未知的威脅和零時差漏洞。
c) 根本原因分析：根本原因分析能顯示導致該次偵測的所有事件。您將可以瞭解該惡意軟體接觸過哪些檔案，協助您有效分析並了解該惡意軟體的來源和經過，以利調整資安政策。
(補充:RCA的功能沒有清除和恢復事件發生前的狀態這個功能)

3. SOHPOS 郵件安全閘道簡介

SOPHOS 郵件安全閘道一直以來都是 SOPHOS 的核心產品線。SOPHOS EMAIL APPLIANCE 是屢次獲得 VB 垃圾郵件防護測試頂級評價的產品。

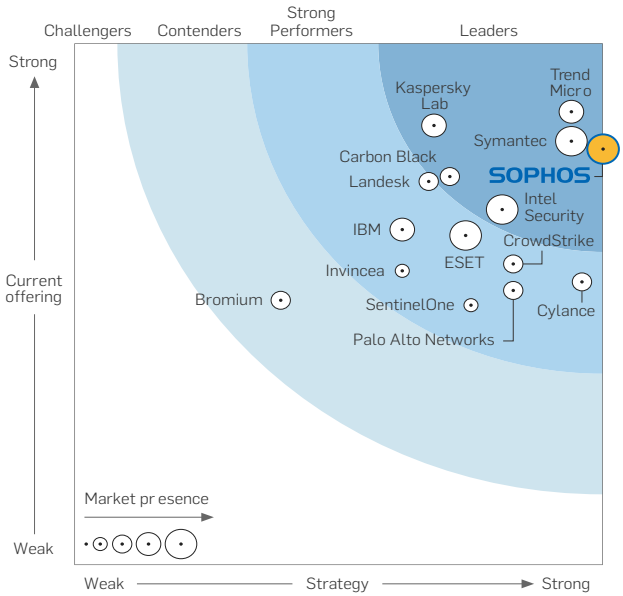


SOPHOS Email Appliance 是一款效能強大，功能豐富的垃圾郵件安全設備，可以旁接部署在使用者網路中，並且支援多種郵件加密方式、病毒郵件防護、垃圾郵件防護和雲端沙箱功能，SOPHOS Email Appliance 產品型號齊全，可以叢集式部署，滿足不同使用者規模的需求，無論是營運商、服務供應商、大型企業或中小企業，均可部署做為垃圾郵件防禦、惡意軟體防禦以及來源於郵件資訊的威脅防禦解決方案。

SOPHOS 有別於其他同業使用 OEM 的防毒引擎，SOPHOS 本身就是傳統的防毒廠商，並連續 8年被評選為企業端點安全的領導者。(圖一)

Forrester Research, Inc. 的最新報告「Forrester Wave™：端點安全套件，2016年第四季」中，將SOPHOS被評定為「領導者」殊榮。Forrester認可SOPHOS在「策略性」類別獲得最高評分。Forrester 認為「在這個創新和傳統端點安全技術環伺的領域中，SOPHOS針對強大的無特徵碼防禦和偵測功能的發展藍圖能讓產品長期擁有高度競爭力。」(圖二)

(圖一)



(圖二)

SOPHOS Email Appliance 設備同時還整合了雲端沙箱，由 SOPHOS 全球威脅回應團隊全年7*24 小時提供服務支援。

當使用者收到一封含有勒索軟體的郵件時，SOPHOS Email Appliance 會對郵件進行全面的檢測， 包括郵件本文內的連結是否惡意，附件是否惡意等等。當 SOPHOS Email Appliance 檢測附件內容為可疑時，會將檔案發往關聯的 SOPHOS Sandstorm 進行確認，如果 Sandstorm 返回結果為 “惡意”， SOPHOS Email Appliance 則將此郵件丟棄，同時發送一封替換的警告郵件給收件人，如果結果為 “正常” 則會將郵件繼續投遞給收件人。由上述內容我們發現，針對勒索軟體的檢測與發現的核心在於基於行為的 Sandstorm 沙箱產品。

Sandstorm採用先進的多層檢測防禦架構，能夠實現快速的回應，大幅降低攻擊風險。文件在進入Sandstorm後會首先經過病毒防護機制的檢測，擁有完整病毒特徵資料的沙箱能夠對可疑檔案進行預先過濾，降低沙箱系統的效能消耗。

隨後，雲端沙箱會對檔案進行掃描，與 SOPHOS Labs 通訊，查詢最新的惡意軟體資訊是否與之匹配，如新特徵碼、IP 信譽、檔案信譽、URL 信譽等等。之後 Sandstorm 會對檔案進行代碼模擬和啟發式檢測。啟發式檢測即沙箱的輕量級檢測，能夠快速定位惡意行為，提高檢測效率。最常用的啟發式檢測是對檔案在限定時間內執行其中的指令或對其程式碼片段進行行為模式分析，然後檢測其中是否包含對系統可能帶來風險的代碼或指令。

Sandstorm 是惡意軟體威脅檢測的利器，APT 攻擊防禦的碉堡。

七、SOPHOS 方案優勢

SOPHOS 向使用者推薦業界獨一無二的勒索軟體解決方案—

Intercept X + Email application

Intercept X 部署在端點 PC 上形成無時無刻的保護。

整合 Sandstorm 雲端沙箱的郵件安全閘道阻斷惡意郵件、釣魚郵件的入侵。
此方案是業界唯一能夠有效對抗勒索軟體的安全方案。其具有以下 3 大優勢：

1. Intercept X基於行為和漏洞的無特徵碼偵測技術識別未知惡意攻擊行為。加密勒索軟體的變化速度快，針對特徵碼偵測的規避機制豐富，這就讓基於特徵碼的防毒和入侵防禦技術在對抗加密勒索軟體時無法起到特別有效的作用。

2. 在加密勒索軟體主要傳播途徑即郵件端進行攔截。SOPHOS Sandstorm 進階威脅防禦系統可根據可疑樣本的行為對其進行評分，進而判定是否為惡意。當有結果後，SOPHOS Sandstorm 會將檢測資訊同步給其他 SOPHOS 安全設備，按照政策進行對應的動作。SOPHOS Email application 更是在郵件安全方面具備業界領先的安全等級和檢測水準。

3. 自動化防禦提升安全回應速度。加密勒索軟體在對抗難度上給防禦方帶來了極大的挑戰，也讓我們發現了傳統安全方案的不足。目前業界很多方案只能提供網路端的安全檢測或郵件安全，或沙箱檢測，互相分割的方案，雖然在檢測方面可能可以達到一定的效果，但是在回應速度方面一定是慢的。SOPHOS勒索軟體解決方案的核心產品 Intercept X 可以和 SOPHOS XG新一代防火牆形成聯合機制，協同工作，不僅針對勒索軟體的傳播特點和技術特點進行強化，更是能夠將防禦、偵測、回應形成自動化作業。在不需人工介入的情況下，將安全回應速度提升到快以秒計。