保安資訊--今日最新(台灣時間2024/04/02)
賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告 (Protection Bulletins)。

關於 保安資訊有限公司 | 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。

在端點啟用賽門鐵克入侵預防系統(IPS)的好處 (以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在 51 萬 5,700 台受保護端點上總共阻止了 5,720 萬次攻擊。這些攻擊中有 84.3% 在感染階段前就被有效阻止：**(2024/04/01)**

- 在**10萬9,600**台端點上，阻止了**1,980**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬6,900**台端點上，阻止了**1,100**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬6,300**台**Windows**伺服主機上，阻止了**8,700**萬次攻擊。
- 在**6萬5,900**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬8,100**台端點上，阻止了**99**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬400**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**17萬7,200**台端點上，阻止了**420**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,300**台端點上，阻止了**420**萬次加密貨幣挖礦攻擊。
- 在**10萬1,900**台端點上，阻止了**770**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**550**台端點上，阻止了**7萬700**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 13 萬 2,700 個受保護端點上阻止了總計 510 萬次攻擊。**(2024/04/01)**

- 使用網頁信譽情資，在 **119.5K** 個端點上阻止 **450** 萬次攻擊。
- 攔截 **28K** 個端點上 **516.6K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **11.3K** 個端點上攔截 **129.6K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **424** 個端點上攔截 **21.8K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

點擊此處獲取--關於賽門鐵克原廠防護週報

2024/04/02
印尼企業成為Agent Tesla網路攻擊行動的目標

賽門鐵克最近觀察到一個個體戶或駭客團體，對準印尼的機構組織進行有針對性的惡意垃圾郵件攻擊行動，儘管在鄰近國家也出現類似情況。這些惡意行為者自稱是印尼一家指標領先的銀行，並採用金融交易社交工程伎倆。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn34
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B!200