保安資訊--今日最新(台灣時間2022/06/27)
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 100 萬個受保護端點上總共阻止了1.921億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/06/19)**

- 在**20萬8,600**台端點上，阻止了**9,350**萬次嘗試掃描**Web**服務器的漏洞。
- 在**41萬3,100**台端點上，阻止了**4,020**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬6,700**台**Windows**伺服主機上，阻止了**1,980**萬次攻擊。
- 在**14萬9,300**端點上，阻止了**860**萬次嘗試掃描伺服器漏洞。
- 在**7萬4,300**台端點上，阻止了**350**萬次嘗試掃描在**CMS**漏洞。
- 在**11萬500**台端點上，阻止了**330**萬次嘗試利用的應用程式漏洞。
- 在**30萬6,700**台端點上，阻止了**820**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,200**台端點上，阻止了**390**萬次加密貨幣挖礦攻擊。
- 在**10萬4,500**台端點上，阻止了**600**萬次向惡意軟體**C&C**連線的嘗試。
- 在**6,600**台端點上，阻止了**28萬1,300**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。

點擊此處獲取--關於賽門鐵克原廠防護週報

2022/06/24

Bronze Starlight 駭客組織利用 HUI 載入程式來部署勒索軟體的有效籌載

據報導，被稱為 "Bronze Starlight" 的駭客組織，在目標網路上散佈勒索軟體，以作為誘餌來分散組織對其活動目的的注意力，其真正目的即有可能竊取機敏資訊。攻擊者一直在利用 HUI 載入程式來大量部署，包括 LockFile、AtomSilo、Rook、Night Sky 和 Pandora 等勒索軟體的有效籌載。這個威脅行為者已知和另一個名為 Bronze Riverside 的駭客組織密切相關的使用各種現成工具，例如：Sodamaster 遠端存取木馬、PlugX 和 Cobalt Strike 來竊取機敏資訊。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Packed.Generic.663
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2022/06/23

中國駭客組織 Tropic Trooper 利用全新的 Nimbda 載入程式來發動攻擊

由中國駭客組織 Tropic Trooper 所發起新的惡意攻擊行動，使用一個被稱為 Nimbda 的新型載入程式和來自 Yahoyah 木馬家族一個全新的惡意軟體。Nimbda 惡意軟體附帶一個 "SMS Bomber"，這是一個可對指定電話號碼發送大量文字訊息的阻斷服務攻擊 (DoS) 類型攻擊的工具。Yahoyah木馬是一個以前被 Tropic Trooperl 濫用的惡意軟體，而這個最新的變種被用來收集本地無線網路的資訊。透過使用圖像隱碼術 (Steganography)，Yahoyah 還植入稱為：TClient 後門是該攻擊行動最終有效籌載。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLoad!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。