保安資訊--今日最新(台灣時間2024/02/17)
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 54 萬 4,900 台受保護端點上總共阻止了 5,230 萬次攻擊。這些攻擊中有 84.6% 在感染階段前就被有效阻止：**(2024/02/12)**

- 在**10**萬**8,100**台端點上，阻止了**1,730**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**14**萬**700**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**8,700**台**Windows**伺服主機上，阻止了**9,300**萬次攻擊。
- 在**6**萬**5,300**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**5,400**台端點上，阻止了**86**萬**9,600**次嘗試掃描在**CMS**漏洞。
- 在**5**萬**900**台端點上，阻止了**120**萬次嘗試利用的應用程式漏洞。
- 在**21**萬**6,500**台端點上，阻止了**460**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,600**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**9**萬**9,400**台端點上，阻止了**690**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**538**台端點上，阻止了**9**萬**6,700**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 15.07 萬個受保護端點上阻止了總計 610 萬次攻擊。**(2024/02/12)**

- 使用網頁信譽情資，在 **135K** 個端點上阻止 **540** 萬次攻擊。
- 攔截 **32.6K** 個端點上 **562.8K** 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 **12.4K** 個端點上攔截 **129.5K** 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 **447** 個端點上攔截 **37.3K** 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

2024/02/16
挖礦劫持惡意程式納入間接系統呼叫規避技術

間接系統呼叫是 Pikabot 等勒索軟體載入程式 (Loader) 經常使用的一種規避技術，最近也觀察到其他類型的惡意軟體也開始採用這種伎倆，最值得一提的是挖礦劫持惡意程式。XMrig 算是挖礦劫持惡意程式圈的老江湖，透過新增 run 註冊表和服務項目來建立常駐功能。然後，它在記憶體中執行，以逃避檢測並在受感染的系統中常駐。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.A!300
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/02/16
RansomHouse駭客組織利用MrAgent工具發動對ESXi平台的攻擊

據瞭解，RansomHouse 駭客組織，過往因利用 WhiteRabbit 或 MarioLocker (又名 Mario ESXi) 等惡意軟體針對 Linux 機器和 VMware ESXi 伺服器進行攻擊而聲名大噪。該駭客組織最近一直在利用一種名為 MrAgent 的工具，該工具允許在大型環境中自動傳遞勒索軟體，並同時透過多個虛擬機管理程式 (Hypervisor) 上部署。MrAgent 具有排程和記錄惡意二進位檔案部署、搜查目標基礎架構資訊以及在虛擬機管理程式 (Hypervisor) 上執行命令的功能。

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(SONAR)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Ransom.Gen
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.C

2024/02/16
Alpha(*阿爾法)勒索軟體

Alpha 是一種全新的勒索軟體，於 2023 年 2 月首次出現，並在最近幾周動作頻繁。它與早已銷聲匿跡的 NetWalker 勒索軟體非常相似，後者在一次國際執法行動後於 2021 年 1 月被剷除。這兩種勒索軟體都採用類似的 PowerShell 載入器來傳遞有效籌載。除此之外，Alpha 和 NetWalker 的有效籌載之間，還存在大量雷同的程式碼。雖然 Alpha 於 2023 年 2 月首次出現，但它一直低調行事，直到最近幾周才似乎開始擴大營運規模並公開一個資料洩漏網站。

在我們的布落格文章中有更詳細的內容：從關門大吉的 NetWalker 崛起，Alpha 搖身一變成為勒索軟體界的後起之秀

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Alpha
- Ransom.Gen
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/02/16
散播DanaBot銀行木馬的垃圾郵件攻擊行動

最近發現一個採用義大利文撰寫的惡意郵件攻擊行動，在散播 DanaBot 殭屍電腦程式。該電子郵件包含一個指向惡意 JS 檔的連結，該檔將會下載並執行 DanaBot DLL。DanaBot 是一種銀行木馬，具有竊取被害人財務資訊的功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Scr.Malcode!gen60
- Scr.Malcode!gen120
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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。

2024/02/16
Srry惡意竊密程式透過惡意JavaScript進行傳播

SrryStealer 是一款全新的惡意竊密程式，它透過惡意 JavaScript 檔，暗中入侵受害者系統。執行後，它會終止目標系統的多個程序，包括與瀏覽器和 Discord 相關的程序。然後，它會收集大量資料，包括系統資訊和個人保存的資料，例如：登錄憑證、瀏覽器歷史記錄、自動填入密碼、信用卡詳細資訊、加密貨幣錢包和 Discord 權杖。收集到的資料隨後會外傳到攻擊者所操控的指揮控制 (C&C) 伺服器。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- 29565_Web Attack: Webpulse Bad Reputation Domain Request

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security，針對此漏洞提供如下的多層級保護：

- 基於可疑程序執行的預防：預防政策可防止惡意軟體在系統中被注入或執行。
- 基於對外連線的預防：在這種情況下，預防政策會阻止網際網路 (mythic-slender[.]online) 的對外連線。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。