保安資訊--今日最新(台灣時間2024/09/30)
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 46 萬 5,200 台受保護端點上總共阻止了 4,660 萬次攻擊。這些攻擊中有 81.3% 在感染階段前就被有效阻止：**(2024/09/23)**

- 在**8**萬**4,700**台端點上，阻止了**1,170**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10**萬**2,800**台端點上，阻止了**830**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3**萬**200**台**Windows**伺服主機上，阻止了**7**萬**3,000**次攻擊。
- 在**5**萬**2,700**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**700**台端點上，阻止了**63**萬**500**次嘗試掃描在**CMS**漏洞。
- 在**5**萬**1,700**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**13**萬**6,800**台端點上，阻止了**560**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1**萬**7,900**台端點上，阻止了**120**萬次加密貨幣挖礦攻擊。
- 在**9**萬**7,300**台端點上，阻止了**750**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**529**台端點上，阻止了**6**萬**9,100**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 7,900 個受保護端點上阻止了總計 400 萬次攻擊。**(2024/09/23)**

- 使用網頁信譽情資，在 **129.1K** 個端點上阻止 **370** 萬次攻擊。
- 攔截 **19.4K** 個端點上 **253.4K** 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 **7.9K** 個端點上攔截 **66.7K** 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 **310** 個端點上攔截 **7.3K** 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

2024/09/29

DCRat(也稱Dark Crystal RAT)特洛伊木馬

DCRa t(也稱 Dark Crystal RAT) 是一款模組化的遠端存取木馬程式，在 2018 年即採用惡意軟體即服務 (malware-as-a-service) 的營運模式問世。它可以執行指令、記錄按鍵和外洩資料。最近，它使用 HTML 挾帶 (HTML smuggling) 這種隱匿手法傳送，在 HTML 中嵌入並混淆有效酬載，以逃避安全軟體的偵測。有效酬載在瀏覽器轉譯／渲染 (Browser Rendering) 時會被啟動，通常需要使用者的互動。Azorult 和 Pikabot 等其他惡意軟體也使用此技術。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Wmi-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.SuspBeh.C!gen2
- SONAR.SuspBeh.C!gen18
- SONAR.SuspBeh!gen313

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen523
- Scr.Malcode.T!gen
- Trojan.Gen.MBT
- 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

2024/09/27

CVE-2024-8190--存在Ivanti Cloud Services Appliance的作業系統指令注入漏洞

CVE-2024-8190 是一個影響 Ivanti Cloud Services Appliance (CSA) 4.6 Patch 518 或更舊版本的高嚴重性 (CVSS 風險評分：7.2) 作業系統指令注入漏洞。若成功開採濫用此漏洞，遠端認證的攻擊者可能會執行任意程式碼。值得注意的是，攻擊者必須擁有管理者權限才能開採濫用此漏洞。此漏洞已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，之前有報告指出此漏洞與另一個 Ivanti 漏洞 CVE-2024-8963 一起被利用在真實網路情境發動攻擊。

網路上的知識：
Ivanti Cloud Services Appliance (CSA) 是一種網際網路裝置，能透過網際網路提供安全的通訊和功能。它充當控制台與受管理裝置，經由他們的網際網路連線進行連結的會合地——即使它們位於防火牆之後或使用代理存取網際網路。

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：

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：

- Web Attack: Ivanti CSA OS Command Injection CVE-2024-8190

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，預設鎖定政策就可保護底層伺服器免受此漏洞影響，包括防止執行任意指令和限制讀取關鍵作業系統檔案。
- DCS 的網路規則政策可設定為，將應用程式限制為受信任的用戶端。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/09/27

知名惡意竊密軟體：Vidar，藉由義大利專用PEC Mail和Telegram個人資料傳播

義大利的 CERT-AGID (類似 TWCERT／CC 台灣電腦網路危機處理暨協調中心) 發現新一起界藉由 PEC 郵箱散佈 Vidar Vidar 惡意竊密軟體攻擊行動。攻擊者仍在利用 Steam 社群設定檔，但一個重要的新策略是利用 Telegram 設定檔。特別是，這些設定檔的個人簡介 (BIOS) 被用來揭露其指揮與控制 (C2) 伺服器的 IP 位址。

網路的知識：

- Steam 社群是由許多熱愛電腦遊戲的玩家所組成。在這裡，您可以找到一起玩遊戲的夥伴、與好友相聚、加入志同道合的群組、主持或加入聊天室，更可參與甚至舉辦大大小小的比賽。
- PEC 郵箱是一款專門為企業量身定制的電子郵件服務，其全稱為『Posta Elettronica Certificata』，意為『認證電子郵件』，是義大利政府推出的一項郵件認證服務。 PEC 郵箱提供安全可靠的電子郵件收發，同時通過獨特的驗證機制，確保郵件內容的合法性和真實性。

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：

自適應防護技術(包含於SESC)：

- ACM.Rgasm-Lnch!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspOpen!gen11

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

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

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。

2024/09/27

Louse進階持續威脅(APT)駭客組織發起針對中國實體的惡意軟體攻擊行動

據報導，Louse 進階持續威脅 (APT) 駭客組織 (又稱為 Patchwork 和 Dropping Elephant) 發起一個針對中國實體的惡意軟體攻擊行動。攻擊手法涉及惡意 LNK 檔案，可能源自網路釣魚電子郵件。此檔案會執行 PowerShell 指令碼，下載誘餌 PDF 和惡意 DLL，並使用 DLL 側載技術。DLL 接著會解密並執行 shellcode，最終部署稱為 Nexe 新最終有效酬載，其目的是從受攻擊的系統中竊取敏感資訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2
- ACM.Ps-Http!g2

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1

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：

- Web Attack: Webpulse Bad Reputation Domain Request

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。