保安資訊--今日最新(台灣時間2025/01/03)
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 31 萬 5,400 台受保護端點上總共阻止了 4,100 萬次攻擊。這些攻擊中有 77.3% 在感染階段前就被有效阻止：**(2024/12/30)**

- 在**7萬1,400**台端點上，阻止了**1250**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬9,700**台端點上，阻止了**620**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,600**台**Windows**伺服主機上，阻止了**6萬4,000**次攻擊。
- 在**4萬5,200**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,000**台端點上，阻止了**80萬500**次嘗試掃描在**CMS**漏洞。
- 在**3萬7,200**台端點上，阻止了**240**萬次嘗試利用的應用程式漏洞。
- 在**6萬7,900**台端點上，阻止了**130**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,500**台端點上，阻止了**84萬1,000**次加密貨幣挖礦攻擊。
- 在**8萬8,800**台端點上，阻止了**860**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**409**台端點上，阻止了**7萬3,000**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 19 萬 1,500 個受保護端點上阻止了總計 690 萬次攻擊。**(2024/12/16)**

- 使用網頁信譽情資，在 **182.3K** 個端點上阻止 **650** 萬次攻擊。
- 攔截 **19.6K** 個端點上 **250.9K** 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 **8.2K** 個端點上攔截 **170.1K** 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 **250** 個端點上攔截 **6.1K** 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

2025/01/02

Nitrogen勒索軟體～被害者乖乖就範就能船過水無痕嗎？

Nitrogen 勒索軟體集團以雙重勒索戰術闖出名號，特別是在過去四個月來非常活躍，目標對象涵蓋建築、金融服務、製造業和科技等不同產業的單位。他們的行動遍及多個國家，特別是在美國、加拿大和英國的影響力尤其強大。

成功入侵後，攻擊者會執行勒索軟體，嘗試終止各種程序、並將加密後的檔案冠上 .NBA 的副檔名，其勒索贖金 (支付) 說明文字檔 (readme.txt) 存放到多個目錄中。它採用反分析技術，例如：偵錯軟體偵測、虛擬機偵測和程式碼混淆 (例如：堆疊字串)。勒索軟體會進行系統搜索，包括列出 PE 區段和收集系統資訊。

他們的勒索贖金 (支付) 說明完全就是威脅性的訊息，目的是迫使受害者就範。劈頭就警告，強調受害者的網路已被加密，敏感資料已被竊取。攻擊者強調情況的嚴重性，威脅如果受害者不回應，就會在他們的暗網部落格上公布被竊資料。他們提出解決方案：解密資料、從伺服器安全刪除被竊資訊，並保證不會讓這件事曝光，但所有條件都以乖乖付款為前提。

該說明強烈不鼓勵尋求第三方解決方案或政府協助，聲稱這些行動會對資料造成無法彌補的損害，或導致 GDPR 法規下的法律和財務懲罰。Nitrogen 還警告說，延遲付款、報警等不好好配合的意圖，將會讓這件事眾所皆知並衍生更多訴訟和嚴重的聲譽損害。

為了更隱密的談判，受害者會被指示使用加密的 Tor 瀏覽器或 qTox 應用程式，透過指定的管道與該組織聯繫。攻擊者承諾會在付款後提供解密工具、資料刪除證明和安全建議，並將自己描繪成專業且掌控一切的人，同時利用恐懼和緊迫感來操縱受害者就範。

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.RansomGen!gen3
- SONAR.Ransomware!g1

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：

- Ransom.Nitrogen
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/12/30

SpyMax手機惡意程式假冒烏茲別克最大的數位服務生態系統：Uzum的手機APP來發動網路攻擊行動

2024 年，惡意行為者假借烏茲別克最大的數位服務生態系統：Uzum 的名義，針對烏茲別克的手機用戶發動一連串的網路攻擊行動。這些攻擊利用 SpyMax(一種偽裝成假冒 Uzum Bank 安卓平台 APP 的知名遠端存取特洛伊木馬程式) 入侵受害者的裝置並竊取敏感資料。

Uzum Bank 是烏茲別克主要的數位銀行，在 Uzum 生態系統中扮演核心角色。這個生態系統整合電子商務、金融科技和銀行服務，以推動全國金融和數位轉型。儘管 Uzum Bank 主要著重於國內服務，但也建立合作夥伴關係，以實現國際交易，進而提高其覆蓋範圍和容易取得性。

在 2024 年 12 月底觀察到的最新網路攻擊行動，突顯濫用 Uzum Bank 信譽的情況。雖然確切的感染手法與途徑尚不清楚，但懷疑惡意簡訊含有下載詐騙 APP 的安裝套件檔 (UzumBank.apk) 之網址，是用來散播惡意軟體。這種方式符合全球威脅份子的常見作案手法，利用可信賴的品牌名稱來引誘受害者。

SpyMax 是涉入這些網路攻擊行動中主要的惡意軟體，是一種複雜的遠端存取木馬程式，主要功能如下：

- 遠端控制遭感染的裝置
- 透過裝置的麥克風和鏡頭進行聲音和影像的擷取
- 竊取簡訊、通話記錄和檔案
- GPS 追蹤以監控受害者位置

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：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Spyware:MobileSpy

2024/12/30

漏洞沒有修補，永遠都是敞開大門的資安破口～Ficora和Capsaicin殭屍網路利用陳年老舊漏洞進行散佈

根據 Fortinet 的研究人員指出，在最近觀察到的網路攻擊行動，有兩個 Linux 殭屍網路 Ficora 和 Capsaicin 出盡鋒頭。這兩個殭屍網路利用數個影響家庭網路管理協定 HNAP(Home Network Administration Protocol) D-Link 老舊漏洞，包括 CVE-2015-2051、CVE-2019-10891、CVE-2022-37056 和 CVE-2024-33112。Ficora 是 Miral 惡意軟體家族中具有 DDoS 攻擊功能的一種，而 Capsaicin 則是 Kaiten 的變種，已知也可用於 DDoS 攻擊。

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：

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：

- CL.Downloader!gen277
- Downloader.Trojan
- Linux.Trojan
- Scr.Malcode!gen107
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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: Malicious Shell Script Download 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。

2024/12/26

Skuld惡意竊密程式持續透過npm(Node Package Manage)的模組倉庫(Registry)以JavaScript開發人員為目標

據報導，有惡意軟體透過 npm(Node Package Manage) 的模組倉庫 (Registry) 部署 Skuld 惡意竊密程式，並以混淆套件針對開發人員為目標。攻擊者上傳惡意套件，例如：windows-confirm、windows-version-check 和 solara-config，偽裝成合法工具，包括常用程式庫和 Solara Python 框架。威脅者使用拚字錯誤的域名手法 (typosquatting) 並利用 Discord webhook 自動訊息以及更新數據機制來進行資料外洩和命令控制 (C&C) 作業。

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-Csc!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1
- SONAR.SuspDataRun

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：

- Backdoor.Ratenjay
- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

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：

- Audit: Bad Reputation Application Activity
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 568

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。

業界公認 **保安資訊**--賽門鐵克解決方案專家

We Keep IT Safe, Secure & Save you Time, Cost

服務電話：0800-381500｜+886 4 23815000｜http://www.savetime.com.tw