保安資訊--本周(台灣時間2025/02/14)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 38 萬 9,000 台受保護端點上總共阻止了 4,560 萬次攻擊。這些攻擊中有 82% 在感染階段前就被有效阻止：**(2025/02/10)**

- 在**8萬3,000**台端點上，阻止了**1,660**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬9,700**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**2萬5,400**台**Windows**伺服主機上，阻止了**560**萬次攻擊。
- 在**5萬3,100**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,900**台端點上，阻止了**84萬9,800**次嘗試掃描在**CMS**漏洞。
- 在**5萬600**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**11萬1,300**台端點上，阻止了**240**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,200**台端點上，阻止了**87萬4,300**次加密貨幣挖礦攻擊。
- 在**10萬4,900**台端點上，阻止了**7萬7,000**台次向惡意軟體**C&C**連線的嘗試。
- 在**480**台端點上，阻止了**6萬800**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 萬 8,400 個受保護端點上阻止了總計 710 萬次攻擊。**(2025/02/10)**

- 使用網頁信譽情資，在 **151.5K** 個端點上阻止 **660** 萬次攻擊。
- 攔截 **18.6K** 個端點上 **306.3K** 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 **6K** 個端點上攔截 **95.6K** 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 **165** 個端點上攔截 **4.9K** 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。

2025/02/14

成軍在2024年的Lynx勒索軟體家族，開始展露頭角

根據 Fortinet 最近一份報告，Lynx 勒索軟體於 2024 年中首次被發現，並被認為是 INC 勒索軟體的接班人。Lynx 已被觀察到針對全球多個產業的 Windows 系統。根據報告，美國的受害者居冠，而加拿大和英國則以較大差距位居第二。約有半數發生在製造業和建築業。

Lynx 包含大多數標準檔案加密勒索軟體常見的功能。功能包括但不限於：

- 只加密特定檔案類型和資料夾，同時排除其他檔案類型和資料夾以加快目標資料的交密速度
- 對應不同的加密等級，會加密目標檔案的 5% 到 100% 不等
- 竊取資料
- 程序和服務終止
- 手動將勒索 (贖金支付) 說明列印到連接的印表機上。

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.Ransom!gen14
- SONAR.Ransom!gen98
- SONAR.RansomPlay!gen1

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。

Carbon Black App Control 在中度或高度強化的預設設定下，具有針對 Lynx 的零時差保護。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Ransom.Zombie
- Trojan Horse
- 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

2025/02/14

Xelera勒索軟體

Xelera 是基於 Python 的勒索軟體家族種，最近在針對印度食品公司 (FCI)(一間公營部門公司) 潛在求職者的行動中散播。攻擊者利用假冒的職務說明／面試通知文件來引誘潛在受害者。該攻擊行動散播 PyInstaller 可執行檔，其中包含 Discord 殭屍與勒索軟體元件。注入的 Discord 機器人主要用於權限升級 (提權)、系統資訊外洩、鎖定系統以及竊取 Web 瀏覽器中儲存的憑證。除了部署 Xelera 勒索軟體元件之外，攻擊者還會利用 MEMZ 駭客工具進行磁碟的 MBR 破壞。

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.Ps-Schtsk!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.Gen
- Trojan.Gen.MBT

- Trojan.KillDisk
- Trojan.Mdropper
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2025/02/14

DEEP#DRIVE攻擊行動

DEEP#DRIVE 是最近發現的惡意攻擊行動，目標是針對南韓的企業、政府單位和加密貨幣持有人。攻擊者利用偽裝成合法文件 (PDF、HWP 或 MS Office 格式)、包含捷徑 .lnk 檔案的壓縮檔網路釣魚電子郵件。後續的攻擊鏈會依賴 PowerShell 腳本的執行、在目標端點建立持久性／常駐，以及下載存在 Dropbox 的有效酬載。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!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：

- CL.Downloader!gen241
- Scr.Mallnk!gen1
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.2
- WS.SecurityRisk.4

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。

2025/02/14

RevivalStone惡意軟體行動部署新的Winnti後繼新變種

一起名為 RevivalStone 的惡意軟體攻擊行動已經被證實，目標是日本製造業和能源業的組織。該攻擊行動是由與中國有關聯的 APT 駭客組織 APT41 所為，該駭客組織持續部署惡名昭章的 Winnti 惡意軟體之最新變種。初始攻擊媒介是利用具有 Web 介面 ERP 系統中的 SQL 注入漏洞，讓攻擊者部署 web shell 並取得初始存取權。一旦進入網路，威脅者就會部署 Winnti 惡意軟體的後繼版本，其功能包含可維持持久性的 rootkit，以及可避免偵測的加密通訊管道。

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-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30

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.Winnkit
- Trojan Horse
- 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

2025/02/14

Destiny Stealer惡意竊密程式

在威脅領域中不乏惡意竊密程式，而 Destiny Stealer 算是一款全新的惡意程式，賽門鐵克正在觀察其測試活動。此惡意軟體是一種普通的惡意竊密程式，目的是從網頁瀏覽器和應用程式擷取登入憑證、滲出特定檔案類型 (例如：文件和影像)，以及竊取 FTP 憑證。與許多其他惡意竊密程式一樣，它也針對 Exodus、Blockchain.com、Binance 和 MetaMask 等加密貨幣錢包為目標

。此外，它還會收集系統資訊、監視剪貼板活動以尋找敏感資料。Destiny Stealer 的手法與最新惡意竊密程式如出一轍，結合了常見的反偵測機制。

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-Wscr!g1
- ACM.Wscr-Wscr!g1
- ACM.Wscr-Ps!g1
- ACM.Untrst-RLsass!g1
- ACM.Ps-Reg!g1

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：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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
- System Infected: Trojan.Backdoor Activity 721
- Web Attack: Webpulse Bad Reputation Domain Request
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 654
- Audit: Untrusted Telegram API Connection

2025/02/13

濫用SmokeLoader惡意軟體發動對烏克蘭銀行業的網路釣魚行動

在真實網路情境上發現濫用 SmokeLoader 惡意軟體，專門針對烏克蘭汽車業和銀行業的網路釣魚行動。其中一個行動目標是烏克蘭最大國有銀行 PrivatBank 的客戶。使用者會受以金融為主題的文件所引誘，例如：虛構的發票和對帳單明細，來引誘落入圈套並入侵系統。此行動濫用內含惡意 JavaScript、VBScript 和 .LNK 捷徑檔案並受密碼保護的壓縮案，以逃避偵測。SmokeLoader 惡意軟體透過程序注入和 PowerShell 執行進行部署，目的是竊取憑證和財務資料，同時維持對受攻擊系統的持續存取。

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-Wscr!g1
- ACM.Wscr-Ps!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。

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：

- Scr.Malarchive!gen7
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C

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。

2025/02/13

程式庫描述檔案(Library-ms)被濫用於近期的惡意垃圾郵件散播行動中

賽門鐵克最近觀察到一個濫用程式庫描述檔案 (Library-ms) 附件的惡意垃圾郵件散播行動。Library-ms 檔案可讓使用者在單一檔案總管中檢視多個目錄的內容。威脅者透過建立合法的本機檔案總管視窗，利用遠端 WebDAV 伺服器，將惡意 .LNK 捷徑檔案散播給毫無戒心的受害者。一旦被執行，就會進一步感染攻擊者預先安排好的其他惡意軟體。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Mallibms!gen1
- WS.Malware.1
- WS.SecurityRisk.4

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。

2025/02/13

CVE-2024-20767--存在Adobe ColdFusion中的路徑遍歷漏洞

2024 年 12 月，美國網路安全與基礎建設安全局 (CISA) 將 Adobe ColdFusion 漏洞 CVE-2024-20767 加入已知漏洞 (KEV) 目錄。此「路徑遍歷」漏洞允許攻擊者繞過路徑名稱的限制，可能導致任意的系統檔案被讀取。此漏洞的 CVSS 風險評分為 7.4，會影響 ColdFusion 2023.6、2021.12 及更早的版本，並需要額外的管理介面才會被開採濫用。資安專家已注意到概念驗證 (PoC) 漏洞利用程式碼的可能性。Adobe 隨後發布即時的安全更新，以緩解這個嚴重等級的漏洞。

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: Adobe Coldfusion Directory Traversal Vulnerability 2

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，可針對 Adobe ColdFusion 應用程式進行安全強化，可採用以下所列的多種不同方式來降低攻擊面和暴險程度：

- 鎖定 Adobe ColdFusion 的網路暴露，使此漏洞或類似的 Adobe ColdFusion 遠端漏洞無法透過公共網際網路被利用。
- 防止存取底層作業系統上的作業系統關鍵檔案，以避免敏感的系統資訊外洩。
- 防止任意程式碼執行，以防止惡意子程序譜系。
- 賽門鐵克的重要主機防護系統：DCS～Data Center Security，預設鎖定政策可保護系統免受此漏洞攻擊，包括防止執行任意指令及限制存取關鍵檔案的讀取。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/02/13

在REF7707網路攻擊行動中發現全新FINALDRAFT惡意軟體

在鎖定南美某國家外交部的 REF7707 網路攻擊行動中，發現一款名為 FINALDRAFT 的全新惡意軟體。該惡意軟體同時有 Windows 與 Linux 的版本，並濫用微軟的 Graph API 服務進行命令與控制 (C&C) 作業。此外，該行動也濫用 PATHLOADER 和 GUIDLOADER 惡意軟體直接在記憶體中下載和執行加密的 shellcode。

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.Untrst-RunSys!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：

- Backdoor.Cobalt
- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.C
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

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

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。

2025/02/13

勒索軟體攻擊中使用與中國有關連的間諜工具

在最近一次針對一家亞洲軟體和服務公司的 RA World 勒索軟體攻擊中，部署通常與中國間諜行為相關的工具。在 2024 年底的攻擊過程中，攻擊者部署一個獨特的駭客工具包，這個駭客工具包之前曾涉入與中國有關聯的威脅行動者用於典型的間諜攻擊。雖然與中國間諜團體相關的工具通常都是共用資源，但許多工具都不公開，而且通常與網路犯罪活動無關。

請參閱我們的部落格：勒索軟體攻擊中使用與中國有關的間諜工具。

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-Rd32!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：

- Hacktool
- Ransom.Babuk
- Ransom.Gen
- Trojan Horse
- Trojan.Gen.MBT

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!100
- 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。

2025/02/12

免錢的永遠最貴～被植入木馬程式的微軟金鑰管理服務(KMS)啟動工具，涉入俄羅斯駭客組織Sandworm的攻擊行動中

根據 EclecticIQ 公司的研究人員所發表的最新報告，俄羅斯國家級駭客組織 Sandworm (也稱為 APT44，UAC-0145) 一直持續針對烏克蘭的使用者發動間諜活動。攻擊者利用被植入木馬程式的微軟金鑰管理服務 (KMS) 啟動工具和偽造的更新安裝程式，散佈新版 BackOrder 惡意程式載入器。此新變種利用各種「就地取材之工具」(LOLbin) 的二進位檔案來逃避防禦。在此行動中散佈的最終有效酬載來自 Dark Crystal RAT (DcRAT) 惡意軟體家族，可被威脅者用於網路間諜及敏感資料外洩。

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-Enc!g1
- ACM.Ps-Http!g2
- ACM.Ps-Net!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Sc!g1

- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-Schtsk!g1
- ACM.Wscr-Msiexec!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.TCP!gen1

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：

- Infostealer
- ISB.Downloader!gen63
- Scr.Malcode!gdn32
- Scr.Malcode!gen120
- Trojan Horse
- Trojan.Gen.6
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!300
- Heur.AdvML.A!500
- 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
- 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。

2025/02/12

小心隨身碟～惡意挖礦程式，透過USB散佈

在韓國，惡意挖礦程式透過 USB 傳播給受害者。除了透過 USB 持續感染外，我們還觀察到後續還會透過修改系統設定和繞過安全機制的手法來獲得更進一步的攻擊成果。特別是 CoinMiner 惡意軟體採用 C&C 伺服器通訊、DLL 側載來執行繞過安全機制的手法、透過 Windows Defender 的排外設定避免被偵測到，以及停用休眠狀態以獲得最佳挖礦效能等手法。

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-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Sc!g1
- ACM.Ps-Schtsk!g1
- ACM.Rd32-Schtsk!g1
- ACM.Rd32-CPE!g1
- ACM.Rd32-RgPst!g1
- ACM.Untrst-RunSys!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：

- PUA.Gen.2
- Trojan Horse
- Trojan.Coinminer
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.3

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
- Heur.AdvML.C

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：

- System Infected: Miner.Bitcoinminer Activity 22

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。

2025/02/11

防護亮點：Telegram和Discord遭濫用於網路攻擊的情況越來越嚴重～安啦！賽門鐵克的用戶

Telegram 和 Discord 遭濫用於網路攻擊的情況越來越嚴重

2024 年，網路罪犯越來越喜歡濫用 Telegram 和 Discord 等合法通訊平台進行資料外洩和其他非法活動。它們擁有廣大的用戶和內建豐富的功能，使其成為吸引未經授權資料傳輸的工具。迄今為止，我們已發佈 184 份與 Telegram 相關的防護公告，以及 121 份與 Discord 相關的防護公告。

在 Telegram 情境裡，威脅份子利用 Bot API 自動從受遭入侵的系統滲出資料。該平台如果遭濫用也會成為散佈惡意軟體的幫兇，目標是敏感的使用者資訊，例如：瀏覽器資料和加密貨幣錢包。此外，Telegram 成為非法市場的重要平台，有專門銷售駭客資料、惡意軟體和非法商品的頻道。聊備一格的內容審查機制和使用者的匿名性更推波助長此一趨勢。網路罪犯也使用 Telegram 進行命令與控制 (C&C) 通訊和通知。

無獨有偶，Discord 的 webhooks 也遭濫用來進行資料外洩，讓網路罪犯可以無縫傳輸所竊取的資訊。其內容傳送網路被濫用來儲存及散佈惡意軟體，將惡意軟體散佈到毫無戒心的使用者身上。和 Telegram 一樣，Discord 也是 C&C 通訊的平台。

背後有多種因素

有幾個因素助長網路威脅在這些平台上的擴散。GitHub 上有多如牛毛的惡意竊密程式--通常都是源於現有惡意軟體的後繼版本--這種方式大大降低攻擊者的技術門檻。免費存取這些工具更讓發動網路攻擊變得更容易。

易於使用和機密性進一步助長了它們遭濫用。Telegram 的加密訊息可讓網路罪犯在保持匿名的同時滲出資料，而 Discord 的 webhooks 則可簡化 C&C 作業和資料竊取。

這兩種平台還能透過 API 來整合包含 Windows、Linux、macOS 和 Android 等跨平台，輕鬆擴展成為自動化的攻擊架構，提高了攻擊的有效性。此外，這兩種平台的廣泛合法使用，讓惡意活動混入正常流量中，使偵測和緩解更具挑戰性。

以 Telegram 和 Discord 為基礎的威脅主要由網路駭客所發動，目標為消費者和企業。這些威脅可能具有高度的目標性或機會性，因此成為全球多個網路犯罪團體和個體戶的萬能工具。

消費者面臨的風險：

- 遊戲：在 Steam、Epic Games 等平台上的帳號和遊戲資產遭竊。
- 加密貨幣：錢包金鑰和交易所認證遭破解，讓攻擊者得以劫取資金。

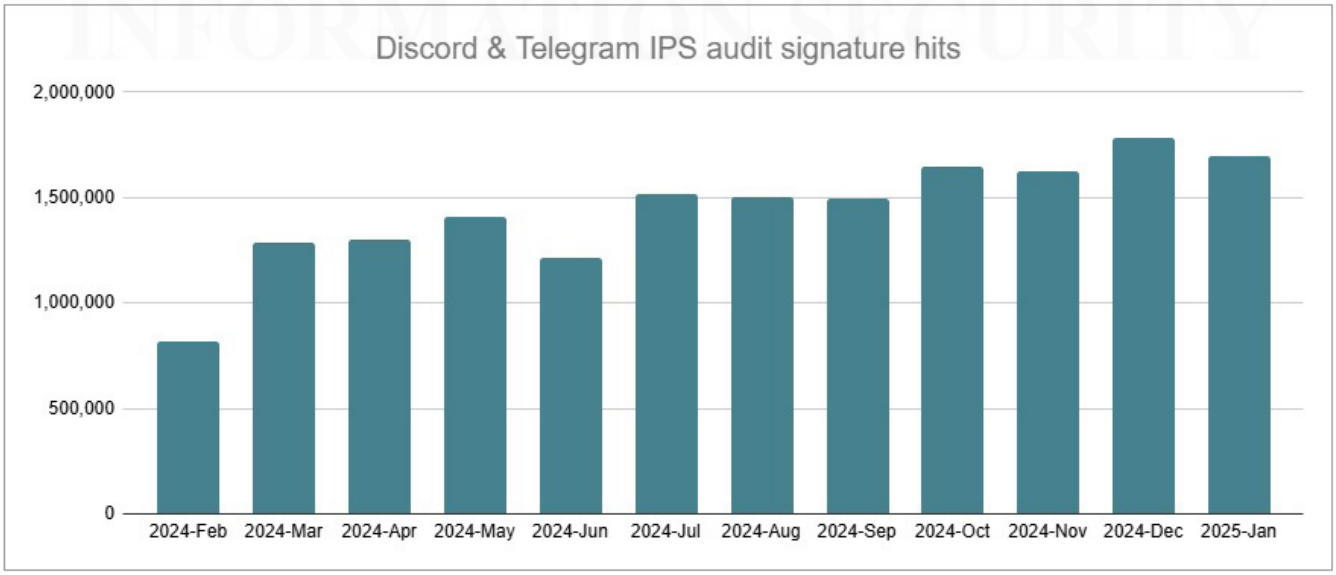
- 檔案：竊取個人檔案 (本機或同步資料夾中儲存的身分證、稅務記錄和敏感檔案)。
- 瀏覽器：竊取儲存的密碼、自動填寫資料、信用卡詳細資料和 cookies。
- 鍵盤測錄：擷取按鍵以竊取密碼、私人對話及其他敏感資料。

企業面臨的風險：

- 企業資料遭竊：合約、藍圖和智慧財產外流。
- 憑證竊取：入侵企業 SaaS 帳戶、電子郵件平台和內部網路。
- 財務開採：使用企業信用卡進行採購或訂閱欺詐。
- 勒索軟體與 IAB：被盜的企業資料可用於索取贖金。或出售給始存取掮客 (Initial Access Broker-IAB) 或勒索軟體集團，為大規模的入侵提供快速取得立足點的情報。

賽門鐵克和 Carbon Black 採用多層次的防護技術能力對抗來自濫用 Telegram 和 Discord 的網路威脅：

- 檔案型防護：進階的行為、啟發式和機器學習防禦技術可在惡意檔案執行之前偵測並攔截惡意檔案。
- 以 EDR 為基礎的防護：Symantec Endpoint Security Complete 和 Carbon Black EDR 可處理與濫用這些服務相關的 MITRE ATT&CK 技術，以及這些威脅使用的許多其他一般 TTPs。
- 政策式保護：Data Center Security 預設政策可針對這些惡意軟體威脅提供零時差保護，防止它們在系統上被注入或執行。
- 網頁式防護：與惡意 Telegram Bots 或 Discord Webhooks 相關的已知網址 (URL) 會進行相對應的分類，以防止使用者存取有害網站，並防止其資料外洩。
- 網路型防護：在 2024 年，賽門鐵克建立數個端點上的網路層入侵防護系統 (IPS) 的稽核特徵，來強化安全性。以下是這些特徵一年的遙測資料：



最初，惡意竊密程式和遠端存取木馬 (RAT) 家族是濫用這些平台的主要惡意軟體。然而，到了 2024 年年中，網路釣魚的型態發生顯著變化。許多網路釣客開始濫用 TelegramBot 來滲出在網路釣魚網頁上輸入的憑證 (閱讀更多內容)。

欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲瞭解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
沒有 SEP？試試使用賽門鐵克瀏覽器防護 (Symantec Browser Protection) 保護您的瀏覽器。
欲瞭解更多關於 Carbon Black 的資訊，請點擊此處。

2025/02/11

與中國有關的駭客濫用BadIIS惡意軟體攻擊IIS伺服器

根據趨勢科技的報告，威脅份子已被發現到以網際網路資訊服務 (IIS) 伺服器為目標，作為佈署 BadIIS 惡意軟體購買搜尋引擎排名 (SEO) 之操弄網路惡意行動的一部分。該行動據信與中國的威脅份子有關，特別以亞洲的伺服器為目標。作為攻擊的一部分，使用者會被重定向至非法賭博網站或惡意軟體或憑證竊取網頁的惡意伺服器，最終目的是獲得財務收益。

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：

- Trojan.Badiis!gen2
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.SecurityRisk.4
- WS.Malware.1

基於機器學習的防禦技術：

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

2025/02/11

Astral Stealer惡意竊密軟體

Astral Stealer 惡意竊密軟體，標榜源於舊版惡意軟體 Hazard Grabber 和 Wasp Stealer 血統。Astral Stealer 用於收集和滲出各種敏感資訊，包括系統資訊、憑證、銀行相關資料、網頁瀏覽器資料、cookies、剪貼簿內容、加密貨幣錢包、第三方應用程式資料、檔案、token等。此惡意軟體具備躲避防毒軟體功能、虛擬機器／沙箱環境感知功能，以及一些持久性／常駐能力機制。收集到的資料可能會透過攻擊者控制的命令與控制通道 (C&C) 或 webhooks 外洩。

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!gen6

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：

- Hacktool
- Infostealer
- Trojan.Gen.MBT
- WS.Malware.1

2025/02/10

SapphireRAT惡意軟體

針對拉丁美洲組織的新一波網路釣魚行動正流行，利用偽造的司法逾期費用收據散佈 SapphireRAT 惡意軟體。威脅者提供如何檢閱和簽署相關文件的詳細指示，試圖增加電子郵件的合法性。然而，這些指示包含一個網頁 (URL)，可將收件者重定向至惡意網站。這個網站是專門設計來上架和傳送 SapphireRAT 惡意軟體，進一步達到攻擊者入侵收件者系統的目的。

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。

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.Gen.MBT
- WS.Malware.1

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。

2025/02/10

FinStealer手機線上銀行惡意軟體

一款全新的手機行動裝置惡意軟體：FinStealer 已在真實網路情境傳出災情。該惡意軟體的二進位檔透過網路釣魚行動或非官方行動應 APP 儲存庫散佈，並偽裝成冒充合法銀行機構的行動 APP。FinStealer 會從受害者身上擷取各種銀行資訊、憑證、信用卡號碼和其他 PII(個人識別資訊)。該惡意軟體以 Kotlin 編碼，Kotlin 是一種與 Java 相容的跨平台高階程式語言。攻擊者透過 Telegram 機器人以及受操控的 C&C 基礎架構擷取所收集的資料。

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。

- Android.Reputation.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。

2025/02/10

SparkCat：跨平台惡意軟體透過Android和iOS上的圖片轉文字(OCR：Optical Character Recognition)攻擊加密錢包

最近有一款名為 SparkCat 的新型惡意軟體，透過官方與非官方應用程式商店針對 Android 與 iOS 使用者進行攻擊，影響範圍遍及歐洲與亞洲。該惡意軟體採用 OCR 技術掃描使用者的圖庫，以尋找加密貨幣錢包的恢復助記詞 (recovery phrase)。它利用 Google 的 ML Kit 進行 OCR，並使用基於 Rust 的自訂通訊協定與指揮控制 (C2) 伺服器通訊。

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：

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：

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

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。

- AdLibrary:Generisk
- AppRisk:Generisk

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。

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，以及基於比原廠更孰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**。