保安資訊--本周(台灣時間2025/02/28)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 37 萬 6,800 台受保護端點上總共阻止了 4,730 萬次攻擊。這些攻擊中有 81.3% 在感染階段前就被有效阻止：**(2025/02/24)**

- 在**7萬9,500**台端點上，阻止了**1,700**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬4,200**台端點上，阻止了**660**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,700**台**Windows**伺服主機上，阻止了**720**萬次攻擊。
- 在**4萬9,300**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,600**台端點上，阻止了**78萬8,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬7,800**台端點上，阻止了**270**萬次嘗試利用的應用程式漏洞。
- 在**10萬6,000**台端點上，阻止了**230**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,600**台端點上，阻止了**83萬9,900**次加密貨幣挖礦攻擊。
- 在**10萬5,200**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**502**台端點上，阻止了**7萬6,200**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 14 萬 8,400 個受保護端點上阻止了總計 770 萬次攻擊。**(2025/02/24)**

- 使用網頁信譽情資，在 **141.6K** 個端點上阻止 **720** 萬次攻擊。
- 攔截 **19K** 個端點上 **336K** 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 **5.7K** 個端點上攔截 **123.2K** 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 **182** 個端點上攔截 **5K** 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。

2025/02/28

LCRYX勒索軟體

LCRYX 是去年在真實網路情境上發現 VBScript 類型的勒索軟體。該惡意軟體會加密使用者檔案，在被加密檔冠上「.lcryx」附檔名，並要求以彼特幣 (Bitcoin) 支付贖金。惡意軟體有能力透過 Windows Management Instrumentation(WMI) 終止重要的系統程序 (例如：工作管理員或登錄編輯程式)。另一項功能會讓它透過發出 PowerShell 指令覆寫磁碟機的 MBR(主開機記錄)。LCRYX 會將惡意 VBS 腳本設定為預設 Shell 以及關鍵系統程序的預設偵錯工具，以確保其在受感染電腦上的常駐／持久性。

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：

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!gen52
- Trojan.Gen.NPE.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。

2025/02/28

Squidoor後門程式最新變種涉入近期的惡意軟體散播行動

Squidoor 是知名模組化的多平台後門程式，支援 Windows 和 Linux 平台。根據 Palo Alto 研究人員指出，此惡意軟體的最新變種散佈在與疑似中國威脅份子有關聯的攻擊中。攻擊者透過利用 Internet Information Services (IIS) 伺服器的已知漏洞，取得目標環境的初始存取權。在初次入侵之後，攻擊者會部署許多惡意的 web shell，允許威脅者執行任意指令並下載額外的檔案。據報導，攻擊者濫用合法的 Microsoft Console Debugger 二進位檔案 (cdb.exe) 來執行 Squidoor 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：

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.Webshell
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- 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。

2025/02/28

最新網路釣魚行動鎖定橫濱銀行的客戶

在日本，橫濱銀行是總部位於橫濱的最大區域銀行。最近，賽門鐵克偵測到新一波假冒橫濱銀行服務的網路釣魚活動，並發出偽造的帳戶通知。這些郵件使用的主旨：【横浜銀行】3月ご利用明細のご案内について (翻譯：【橫濱銀行】3月份交易明細資訊)。電子郵件內容簡短，鼓勵收件人點選並檢視每月交易明細。按一下電子郵件內的連結，收件者就會被重導向到偽造的橫濱銀行登入頁面，以竊取憑證。一旦遭入侵，攻擊者就可以存取受害者的橫濱銀行帳戶。

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)。

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。

2025/02/27

Billbug(又名Lotus Blossom)威脅組織使用Sagerunex惡意軟體大肆攻擊

Billbug (又名 Lotus Blossom) 威脅組織已被發現利用 Sagerunex 惡意軟體以及其他駭客工具，針對各產業的眾多受害者發動攻擊。在 Cisco Talos 研究人員最近一份報告中，該組織攻擊活動影響亞洲的政府、製造業、電信與媒體等組織。Sagerunex 是一個已知由惡意 DLL 組成的後門軟體，可從記憶體注入並直接執行。

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：

- Backdoor.Sagerunex
- Hacktool
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

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

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。

2025/02/27

新一波網路釣魚攻擊鎖定日本知名的大型連鎖購物中心Yodobashi Camera(日語：ヨドバシカメラ：友都八喜)的客戶

在日本，Yodobashi Camera Co., Ltd(日語：ヨドバシカメラ：友都八喜) 是一家大型零售連鎖店，主要銷售電子產品、個人電腦、相機和攝影器材。最近，賽門鐵克觀察到新一波偽冒 Yodobashi Camera 服務的網路釣魚活動。電郵內容提及客戶資料已更改，並誘使用戶點擊釣魚網

址以確認更改。點擊電子郵件中的連結會將用戶重導向到偽造的 Yodobashi Camera 登入頁面，目的是竊取憑證。

電子郵件標頭：

- 電子郵件主旨：Yodobashi.com：「お客様情報」変更依頼受付のご連絡_ID:[random_12_digits]
- 翻譯後的電子郵件主旨：Yodobashi.com：「客戶資訊」變更要求通知 ID: [random_12_digits]

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)。

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。

2025/02/27

Vedalia進階持續威脅(APT)駭客組織在亞洲發動散播RokRat 惡意軟體的大規模網路釣魚行動

據報導，與北朝鮮有關聯的駭客組織：Vedalia(也稱為 APT37、RedEyes 和 ScarCruft) 所發起的網路釣魚行動會傳送無檔案型態 (Fileless) 的 RokRat 惡意軟體。該攻擊行動目標是南韓和亞洲各地的政府和企業單位。攻擊媒介包括含有惡意捷徑檔 .LNK 的 ZIP 壓縮附件檔的電子郵件，這些檔案會偽裝成北朝鮮事務、外交政策或貿易協定的文件。當執行時，.LNK 檔案會觸發多階段的攻擊，最後以 RokRat 作為最終的有效酬載。從雲端的有效酬載轉變至獨立的 .LNK 檔案，顯示 Vedalia 能適應不斷演進的安全防禦。

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.Powershell!g20

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：

- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.NPE
- 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。

2025/02/26

LightSpy：針對社交媒體的全新多平台間諜軟體

據報導，LightSpy 間諜軟體的後繼新版本支援多平台也擴充指令功能清單。它已將重點從訊息應用程式轉移到從 Facebook 和 Instagram 等社交媒體平台擷取資料，包括訊息、聯絡人和帳號元資料。Windows 版本擁有更強大的功能，包括鍵盤側錄、錄音、視訊擷取和 USB 互動，反映出從純資料收集轉向更廣泛的作業控制和系統監控。

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：

- Trojan Horse
- Trojan.Maljava
- WS.Reputation.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。

2025/02/26

安卓平台上的TgToxic惡意軟體出現最新變種

TgToxic 是一款安卓平台上的惡意竊密軟體，最早是透過釣魚網站和遭入侵的社交媒體帳戶傳播。最新出現的 TgToxic 惡意軟體最新變種透過惡意簡訊傳送。更新的功能包括使用網域產生演算法來建立全新的 C&C 網址，用來傳送竊取的資料，並改善檢查以確保惡意軟體是在實際的安卓平台裝置上執行。TgToxic 現在還可以透過偽裝成 Google Chrome 隱藏在遭入侵的 Android 手機上，因為它使用相同的圖示和名稱，這樣受害者就不太可能嘗試將其從裝置中移除。

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.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。

- 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。

2025/02/26

Snake鍵盤側錄惡意程式出現最新的變種

已觀察到針對 Windows 使用者的 Snake 鍵盤側錄惡意程式 (又稱為 404 鍵盤側錄惡意程式) 出現最新的變種。Snake 鍵盤側錄惡意程式通常透過含有惡意附件或網址的釣魚郵件進行傳播。它會針對主流的網頁瀏覽器 (例如：Chrome、Edge、Firefox 等) 監控／記錄按鍵。此新變種採用 AutoIt (一種常用於在 Windows 環境中自動執行任務的腳本語言) 來傳送和執行其惡意有效酬載。執行時，它會注入一份自身的複本，將其屬性設定為隱藏，以便隱身不被發現。它會擷取敏感資訊 (例如：憑證)，然後將其滲出到 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：

自適應防護技術(包含於SESC)：

- SONAR.Trafic2.RGC!g16

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.Malcode!gen
- Trojan.Gen.MBT
- Trojan.Malautoit!g*
- 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。

2025/02/26

假冒日本宅配業者：Sagawa(佐川急便)的網路釣魚行動專門鎖定憑證(帳／密)

賽門鐵克發現新一波的網路釣魚攻擊，假冒日本宅配業者：Sagawa (佐川急便) 專門鎖定憑證 (帳／密)。在這一波攻擊中，釣魚電子郵件偽裝成送貨通知，要求立即更新送貨地址。電子郵件內容簡短，鼓勵收件人點選釣魚網址。一旦點選，受害者就會被導引到專為蒐集憑證而設計的網頁。

電子郵件標頭：

- 電子郵件主旨：【重要】住所不備による配送不能のお知らせ/[Urgent] Delivery Suspension Notice FN-26983986185
- 翻譯後的電子郵件主旨：[重要]因地址不完整導致配送失敗的通知/[緊急]暫停配送通知 FN-26983986185

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)。

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。

2025/02/26

透過SalmonSlalom網路攻擊行動散佈的FatalRAT惡意軟體

代號：SalmonSlalom 的網路攻擊行動專門鎖定亞太地區 (APAC) 的工業組織。攻擊者一直在利用各種第一和第二階段的惡意程式載入器，其最終的目的就是導致 FatalRAT 最終有效酬載的感染。雖然 FatalRAT 惡意軟體在過去已經散布好幾次，但據報導這次攻擊行動散布是此惡意軟體家族的最新版變種。FatalRAT 具備執行各種惡意動作的功能，例如：

- 從受感染的機器收集資訊
- 執行鍵盤側錄
- 擷取並執行從攻擊者端接收的指令
- 刪除已遭入侵端點上的資料夾和使用者資料
- 任意檔案下載與執行
- 啟動和停止各種系統程序等

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- 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：

- Trojan.Gen.2
- Trojan.Gen.MBT
- Web.Reputation.1
- Web.Reputation.3
- 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
- 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。

2025/02/26

冒牌的DeepSeek網站用來大肆散播惡意軟體

最近有許多以 DeepSeek 為主題的惡意軟體散播行動正在上演。DeepSeek 是最近發布的人工智能聊天機器人，與大家耳熟能詳的 ChatGPT 非常相似。攻擊者利用 DeepSeek 品牌的日益普及，建立大量假冒 DeepSeek 網站和外觀相似的網域名稱，用於提供惡意有效酬載。最近一次攻擊行動就是向毫無戒心的 macOS 使用者傳送 Poseidon Infostealer惡意竊密軟體。另一種攻擊則是向受害者散佈 Vidar Stealer 惡意竊密軟體。攻擊者主要利用這兩種惡意軟體家族來滲出各種敏感資料，包括憑證、個人檔案、瀏覽器資料、加密錢包等。

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!g5
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- Trojan.Gen.MBT

- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- 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。

2025/02/26

鎖定日本全日空ANA哩程俱樂部會員的全新網路釣魚行動

賽門鐵克發現一個針對日本用戶的網路釣魚行動，該行動濫用偽造全日空 (ANA) 電子郵件。這些郵件的主旨類似：「ANAマイレージクラブ重要なお知らせ--事後登録手続きのお願い」。

(翻譯：「全日空飛行紀錄俱樂部重要通知--申請補辦註冊手續」(ANA Mileage Club Important Notice--Request for Retroactive Registration Procedure)

網路釣客濫用會員熟悉的「補辦註冊手續」程序，讓會員申領過往航班的哩程積分。這使得電子郵件看起來合法且與飛行常客相關。按下電子郵件內連結後，使用者就會被轉到偽造的全日空登入頁面，以竊取憑證。一旦遭入侵，攻擊者就可接管受害者的飛行哩程俱樂部帳戶。

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)。

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。

2025/02/26

代號：Ghostwriter 的網路攻擊行動最新行蹤

Ghostwriter 是專屬於 UNC1151(UAC-0057) 威脅組織的網路攻擊行動代號。據了解，該網路攻擊行動至少從 2016 年就開始積極運作，最新行踪大約在 2024 年 11 月至 12 月期間被觀察到。據報導，此行動針對烏克蘭的軍事和政府組織，以及白俄羅斯的社運人士。已知初始攻擊源於攻擊者會濫用包含惡意 VBA 巨集的 Excel 文件檔。後續的感染鏈會執行稱為 PicassoDownloader 惡意程式下載器，此惡意程式也曾出現在該威脅組織的早先攻擊行動中。

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.MSExcel!g4
- SONAR.MSExcel!g6
- SONAR.MSExcel!g11

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!gen68
- ISB.Downloader!gen433
- ISB.Dropper!gen1
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.Malware.2

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。

2025/02/25
防護亮點：端點防護--SEP多重防護技術中的入侵預防系統元件(IPS)去年(2024 年)您做了什麼?

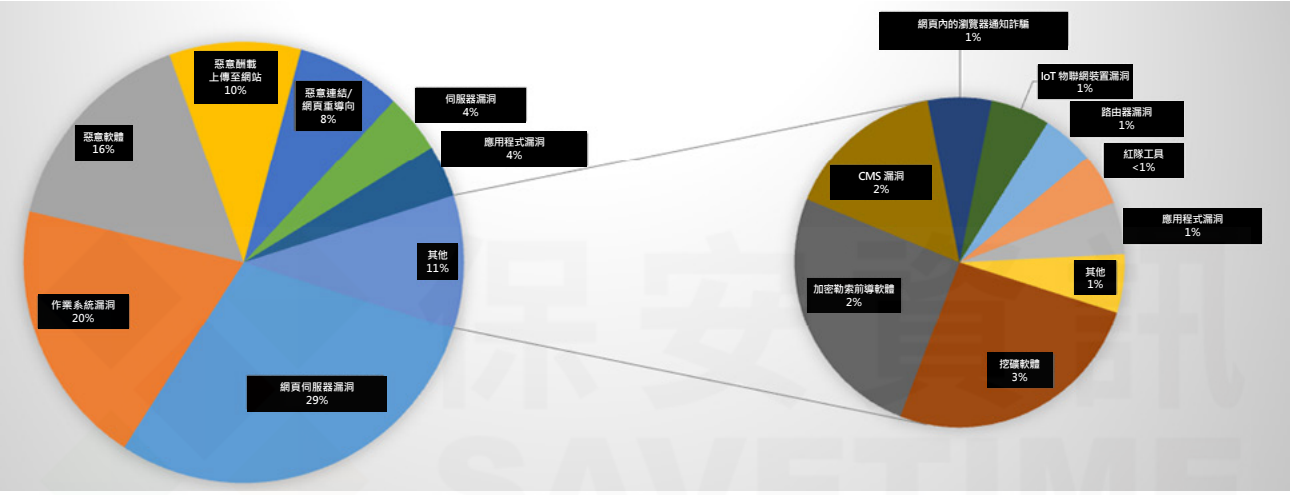
賽門鐵克的 IPS 是同類最佳的深度資料封包檢測引擎，可保護包括財富 500 強企業和消費者在內的數億個端點 (桌上型電腦和伺服器)。我們曾多次發布介紹在防禦態勢中使用 IPS 的好處--從攔截技術支援詐騙，到制止無休止的 Log4j 攻擊，再到網路釣魚、SMB 攻擊、CMS 漏洞、高效的 IPS 瀏覽器擴展等，不一而足。引用上一篇文章中的評論：「如果您的安全設置不包括入侵防禦，那麼您的組織就有可能在威脅防護方面遭受重大損失」。

讓我們回顧過去的一年， 看看 IPS 如何協助保護我們的客戶。

在 2024 年期間，SEP 的多重防護技術中，單單入侵預防系統元件 (IPS) 的網路防護引擎在賽門鐵克保護的端點上攔截超過 **27 億次威脅**。**其中 92% 的攻擊**在感染前階段就被攔截。

- 利用網路伺服器漏洞的嘗試：29%
- 企圖利用 Windows 作業系統漏洞：19%
- 惡意軟體 C&C 連線嘗試：16%
- 試圖執行 Web 有效載荷上傳： 10%
- 試圖將用戶重導向到攻擊者控制的網站：8%
- 試圖利用伺服器漏洞：4%
- 試圖利用應用程式漏洞：4%
- 其他：10%。

SEP 的入侵預防 (IPS) 防護技術所阻擋的威脅數量 (2024)



建議客戶在桌機／筆電和伺服器上啟用 IPS，以獲得最佳保護。點擊此處瞭解啟用 IPS 的說明。欲了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。

2025/02/24

SectopRAT遠端存取木馬(RAT)，偽裝成Chrome瀏覽器的安裝程式來散播

SectopRAT 遠端存取木馬 (RAT)(也稱為 ArechClient2) 是一款基於 .NET 多功能惡意竊密程式，用來竊取受害者機器上的敏感資訊。在真實網路情境上已經觀察到散播此惡意軟體的新一波行動。攻擊者最近將其偽裝成 Google Chrome 瀏覽器安裝程式，透過濫用 Google Ads 平台散佈此多功能惡意竊密程式。

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-Msbuild!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen804

- SONAR.SuspLaunch!g349
- SONAR.SuspLaunch!g444
- SONAR.SuspPE!gen32

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：

- Downloader.Trojan
- 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

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: Bad Reputation Application Connecting to Cloud Storage
- System Infected: Trojan.Backdoor Activity 812
- 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。

2025/02/24

惡意捷徑檔. LNK被用作惡意行動的工具，鎖定教育機構的散播Lumma惡意竊密程式

據報導，有惡意軟體利用教育機構的基礎架構散佈 Lumma 惡意竊密程式。此攻擊始於偽裝成 PDF 文件的惡意捷徑檔. LNK，來引誘受害者。一旦執行，這些檔案會觸發後續多階段的感染鏈，最終在遭駭入的系統上部署 Lumma 惡意竊密程式。此惡意軟體的目標是敏感資料，包括密碼、瀏覽器資訊和加密貨幣錢包的詳細資訊。惡意軟體使用先進的迴避技術，例如：利用 Steam 設定檔進行 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-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Wmic-Http!g1
- ACM.Wmip-Mshta!g1
- ACM.Wmip-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：

- CL.Downloader!gen111
- Scr.Heuristic!gen20
- Scr.Mallnk!gen10
- Scr.Malcode!gen
- Scr.Mallnk!gen13
- Trojan.Gen.MBT
- Web.Reputation.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。

2025/02/23

流行趨勢是很好的釣餌～偽裝成ChatGPT訂閱通知的網路釣魚行動

在賽門鐵克最近觀察到網路釣魚行動中，偽裝成「每月續訂」通知的電子郵件正大肆傳送給目標收件者。主旨通常包含「action required」(需採取行動) 或「Reminder」(提醒) 等關鍵字，這是引誘收件者開啟電子郵件的常用手法。電子郵件的本文宣稱需要每月支付 24 美元的訂閱費才能使用 ChatGPT 的進階功能。若要完成付款，收件者會被提示點擊一個目的在竊取其憑證的網路釣魚網址。電子郵件標頭如下：

- Subject：Action Required: Secure Continued Access to ChatGPT with a $24 Monthly Subscription
  From:ChatGPT <假冒的郵件信箱>。

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)。

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。

2025/02/21

Core勒索軟體--源於Makop的後繼最新變種

Core 勒索軟體是源於 Makop 的後繼最新變種，最近已經出現在真實網路情景上。該勒索軟體會加密使用者檔案，並冠上 .core 副檔名。受害者的編號和開發者的電子郵件地址也會附加到副檔名中。該勒索軟體會以檔名為「README-WARNING.txt」的文字檔形式留下勒索 (贖金支付) 說明。Core 還具有刪除受遭駭端點上的陰影副本和備份資料的功能，以及修改登錄檔機碼取得常駐功能。

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：

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.Makop!g1

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.B!200

2025/02/21

Ghost(也稱為Cring)勒索軟體

賽門鐵克的安全機制應變中心 (Symantec Security Response) 得知美國網路安全暨基礎設施安全局 (CISA)、聯邦調查局 (FBI)、各州資訊共享及分析中心 (MS-ISAC) 針對勒索軟體 Ghost (也被叫做 Cring）最新一波攻擊提出警告，指出這些駭客通常會對於提供網際網路服務的應用系統已知漏洞下手，從而入侵並以勒索軟體加密檔案。這個勒索軟體家族的幕後指使者濫用已公開揭露的漏洞，試圖開採提供網際網路服務伺服器的弱點。開採濫用下列 (但不限於) CVE-2018-13379、CVE-2010-2861、CVE-2009-3960、CVE-2021-34473、CVE-2021-34523、CVE-2021-31207 等陳年

漏洞。

根據已發佈的警告，Ghost／Cring 勒索軟體至今已入侵超過 70 個國家的各行各業。已部署的勒索軟體有效酬載會加密使用者檔案，隨附的勒索 (贖金支付) 說明有些還會特別註明可能會外洩使用者的機敏資料。攻擊者在攻擊中使用 Cobalt Strike 和許多開放原始碼工具，包括 IOX、SharpZeroLogon、BadPotato 等。

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-Net!g1
- ACM.Ps-Sc!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.TCP!gen1
- 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.Iox
- PUA.Gen.2
- Ransom.Gen
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- 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!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：

- Web Attack: ColdFusion Remote Code Exec CVE-2010-2861
- Web Attack: Fortinet FortiOS Directory Traversal CVE-2018-13379
- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473

2025/02/21

喬裝成xigncode反作弊程式的惡意程式有XWorm惡意程式的特質

最近，有人發現偽裝成 xigncode 反作弊程式的可執行檔的惡意軟體樣本。XingCode 是線上遊戲常用的反作弊軟體，用來防止作弊、駭客入侵和未經授權的第三方工具。這些惡意檔案包含內嵌的 PowerShell 腳本，用於對資料進行去混淆處理。這些檔案展現出 XWorm 惡意軟體的特質，具有系統操控、資料外洩和鍵盤記錄等功能，意在建立常駐／持久性和逃避偵測。

XWorm 是一種基於 .NET 的商品化遠端存取木馬 (RAT)，在真實網路情境被廣泛操弄。雖然該惡意軟體家族在過去曾多次被發現，但新版本仍在地下論壇上出售，並可能由不同的威脅組織在不同的攻擊行動中大肆傳播。除了典型 RAT 常見的功能外，XWorm 最新變種還具有一些額外的竊密功能，允許攻擊者收集機密的使用者資料、銀行詳細資訊、憑證、cookie 和其他資訊。該惡意軟體還可以從 C&C 伺服器下載其他外掛程式，從而進一步增強其運作能力。

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-Schtsk!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-FlPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen93
- SONAR.SuspBeh!gen752

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.Heuristic!gen5
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.SecurityRisk.4

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.B!200

2025/02/20

散播Rhadamanthys惡意竊密程式的攻擊行動濫用Microsoft管理控制台(MSC)檔及操作視窗被用來傳播惡意軟體

自 2024 年年中以來，MSC 惡意軟體涉入的惡意行動日益增多，並發現有人濫用 CVE-2024-43572 Microsoft Windows Management Console 遠端程式碼執行 (RCE) 漏洞進行攻擊。已觀察到一個散佈 Rhadamanthys 惡意竊密程式的攻擊行動，該惡意軟體偽裝成 MSC 檔案。新發現的 MSC 檔案屬於透過 Console Taskpad 執行「command」指令的惡意程式。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspStart!gen14

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
- Trojan Horse
- 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.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: Microsoft Management Console CVE-2024-43572 Download

2025/02/20

奈及利亞威脅份子散佈XLogger惡意軟體

奈及利亞威脅份子的惡意軟體攻擊行動已被觀察到散佈 XLogger 惡意軟體。此行動始於使用 Google dorking 伎倆收集電子郵件位址，並建置偽造的網站在不法業者所提供防彈代管服務上。使用者會被透過 ChatGPT 製作的釣魚電子郵件誘騙，其中包含可執行檔案的 RAR 壓縮附件。執行後，PowerShell 指令碼會解密惡意軟體的有效籌載，用將竊取的資料滲出到 Telegram 頻道。

網路上知識：

谷歌駭侵法 (Google hacking)，也叫 Google dorking，是一種利用谷歌搜尋和其他谷歌應用程式來發現網站配置和程式碼中的安全漏洞之駭客伎倆。

防彈代管 (bulletproof hosting)，泛指網站服務業者所提供主機位於司法比較不嚴謹的地區，執法與查核有相當的困難度，這種服務特別受到非法服務的喜愛。

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。

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：

- Packed.NSISPacker!g19
- Scr.Malcode!gen

- 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。

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**。