保安資訊--本周(台灣時間2025/08/22)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 32 萬 6,400 台受保護端點上總共阻止了 4,430 萬次攻擊。這些攻擊中有 80.5% 在感染階段前就被有效阻止：**(2025/08/18)**

- 在**6萬8,900**台端點上，阻止了**1,760**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**6萬4,900**台端點上，阻止了**500**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**1萬9,900**台**Windows**伺服主機上，阻止了**490**萬次攻擊。
- 在**4萬1,800**台端點上，阻止了**150**萬次嘗試掃描伺服器漏洞。
- 在**1萬100**台端點上，阻止了**66萬9,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬700**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**7萬3,100**台端點上，阻止了**210**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,100**台端點上，阻止了**68萬5,900**次加密貨幣挖礦攻擊。
- 在**9萬2,700**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**544**台端點上，阻止了**7萬7,700**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 26 萬 7,200 個受保護端點上阻止了總計 1,250 萬次攻擊。**(2025/08/18)**

- 使用網頁信譽情資，在 **255.7K** 個端點上阻止 **11.4M** 次攻擊。
- 攔截 **32.7K** 個端點上 **971.5K** 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 **6.1K** 個端點上攔截 **143K** 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 **367** 個端點上攔截 **9.4K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 攔截 **728** 個端點上的 **4.8K** 次技術支援詐騙攻擊
- 在 **187** 個端點上阻止 **3.7K** 次加密劫持嘗試

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。

2025/08/21

冒充多個組織的VIP Keylogger鍵盤側錄程式的傳播行動

賽門鐵克最近觀察到一連串傳播 VIP Keylogger 鍵盤側錄程式的惡意電子郵件，攻擊者冒充物流、工程和製造等行業的多個合法組織，利用一般的採購訂單、報價單、出貨通知和銷售合約進行社交工程誘騙。

攻擊鏈遵循熟悉的模式：電子郵件→檔案→可執行檔案。收件人被誘騙開啟高可信度的ZIP壓縮檔，文件的檔名令人信服，例如：「PURCHASE ORDER.zip」、「Signed and stamped sales contract.zip」或「QUOTATION.zip」。檔案內包含偽裝成合法文件的可執行檔，執行時會部署 VIP Keylogger 鍵盤側錄程式。

目標橫跨多個地區和產業，英國、西班牙、法國、荷蘭、瑞士、比利時、模里西斯、印度、巴西、波札那、加納和貝南的組織都收到這些電子郵件。受害行業包括物流、能源、政府機構、金融、旅遊、醫療保健和消費品。

觀察到的電子郵件主題：

- AIR SHIPMENT// SGN-FRA// BORG WARNER / Part number# 53031504457 /// SGN47979941
- Spares shipment LCL to Shanghai—17/8/2025
- PO234937 QUICKLIME 90% CaO
- QUOTATION: Prodigy // Austalis // AE Service kits
- QUOTATION JUNNE - SANSA 03/06/2025 (WINOX)
- SALES CONTRACT FOR ORDER #2523405 VIP Keylogger

安裝 VIP Keylogger 鍵盤測錄程式後，攻擊者就能擷取鍵盤按鍵、竊取憑證和滲透敏感資訊，進而進行後續欺詐或更深入地入侵企業網路。

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：

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.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.Gen.2
- Scr.Malcode!gdn34

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/08/21

惡意垃圾郵件以銀行主題誘騙，土耳其各行各業正遭受散播Snake Keylogger鍵盤側錄程式的攻擊

賽門鐵克最近發現一個假冒土耳其主要金融機構散佈 Snake Keylogger 鍵盤側錄程式的惡意垃圾郵件攻擊行動。攻擊者精心製作仿冒合法金融通訊的網路釣魚電子郵件，使用「686,84 EUR Swift Bildirimi」等主題和仿冒官方網域的偽造寄件者地址。

惡意攻擊鏈以一封傳送壓縮 .Z 檔案附件的電子郵件開始，該附件名為「[銀行名稱] Bnakasi swift Mesaji.pdf.z」。受害者會在裡面找到看似 PDF 的檔案，但實際上是以誤導性名稱偽裝的可執行檔案：「[銀行名稱] swift Mesaji.exe」。啟動時，該可執行檔會安裝 Snake Keylogger，這是一款著名的竊取惡意軟體，專門用於擷取敏感資訊，例如：憑證、擊鍵和系統資料。

對目標收件人的分析顯示出受害者的多樣性。此行動的對象包括在土耳其經營食品和物流業的公司、歐洲的能源公司，以及德國、巴哈馬和土耳其的遊輪港口業者。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

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)。

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：

- MSIL.Packed.19
- Trojan.SnakeKeylogger

基於機器學習的防禦技術：

- Heur.AdvML.B

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: TLS v1 Request
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 654

2025/08/21

Crypto24威脅組織最近的活動包括部署RealBlindingEDR工具

據觀察，名為 Crypto24 威脅份子最近針對各行各業的知名組織進行多階段攻擊。根據趨勢科技研究人員的報告，該威脅組織利用自訂惡意軟體、各類合法工具和多個就地取材二進位檔案 (LOLBins) 進行活動。在部署的工具包中，攻擊者使用自訂的 RealBlindingEDR 版本，這是一款開放源碼 EDR 繞過工具，設計的唯一目的是迴避和停用安全軟體。Crypto24 所進行的攻擊行動目的在持續遠端存取被入侵的系統、監視以及資料蒐集和滲透。

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-Rd32!g1
- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Sc!g1
- ACM.Ps-SvcReg!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspDriver!g10
- 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。

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 針對 RealBlindingEDR 的戰術、手段、流程 (TTP) 所設計的 EDR 強化規則包括：
  - Command and Scripting Interpreter [T1059]
  - Command and Scripting Interpreter: Visual Basic [T1059.005]
  - Command and Scripting Interpreter: JavaScript [T1059.007]
  - Exploitation for Privilege Escalation [T1068]
  - Ingress Tool Transfer [T1105]
  - Masquerading: Masquerade File Type [T1036.008]
  - Modify Registry [T1112]
  - Query Registry [T1012]
  - Software Discovery: Security Software Discovery [T1518.001]
  - Subvert Trust Controls [T1553]
  - Windows Service [T1543.003]
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2

- Trojan.Gen.6
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.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!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。

2025/08/21

OSGeo/GeoServer/GeoTools存在高風險安全漏洞(CVE-2024-36401)在最近的資源變現型攻擊行動中遭濫用

根據 Palo Alto Networks 最新報告，在真實網路情境上發現一起濫用遠端執行程式碼 (RCE) 漏洞：CVE-2024-36401 的全新攻擊行動。此漏洞影響 OSGeo GeoServer GeoTools 產品，它是一個 Java 語言的開放源碼軟體，可讓使用者分享及編輯地理空間資料。威脅者在存取有漏洞的系統後，會嘗試部署軟體開發套件 (SDK) 及修改應用程式。攻擊者的目標是將受害者的網際網路頻寬利潤化，進而從被攻擊系統中獲得被動的收入來源。

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：

- Downloader
- Linux.Trojan
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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: GeoServer RCE Vulnerability CVE-2024-36401
- Web Attack: GeoServer RCE Vulnerability CVE-2024-36401 2
- Web Attack: GeoServer RCE Vulnerability CVE-2024-36401 3

基於安全強化政策(適用於使用DCS)：

- Symantec Data Center Security (DCS) UNIX 強化防護政策可設定為停用反向連線、允許已建立的相關連線，以及僅允許 DNS、HTTP 和 HTTPS 等必要的離埠流量。
- 客戶也應停用 WFS 請求，直到將 GeoServer 升級至已修補的版本。

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。

2025/08/21

出現全新惡意程式載入器：SoupDealer

SoupDealer 是最近在真實網路情境上發現到一種全新的惡意程式載入器，目標是土耳其的使用者。此惡意軟體以 Java 撰寫，透過惡意垃圾郵件行動中的惡意 .jar 附件散佈。SoupDealer 利用 TOR 加密網路進行 C&C 通訊。惡意軟體執行後，會使用持久性、工作排程、提權，以及偵測和迴避沙箱的技術。SoupDealer 可讓攻擊者截圖、發起 DDoS 攻擊、執行遠端指令或下載額外的任意有效酬載等。

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：

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。

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID
- 賽門鐵克的端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Maljava

2025/08/21

新版DarkCloud所涉入的最新竊密行動驚覺其已採用ConfuserEx的混淆手法

來自 Unit 42(Palo Alto Networks) 最新威脅報告強調傳播 DarkCloud 惡意竊密程式的感染鏈已經大進化，現在使用 ConfuserEx 進行混淆，並以 Visual Basic 6 寫成最後的有效酬載。自 2025 年 4 月以來，已觀察到至少三種被散播的新變種，都是以釣魚電子郵件開始，電子郵件含有執行 JavaScript 或 Windows Script Files 的壓縮檔案 (.TAR、.RAR 或 .7Z)。這些腳本會取得並執行 PowerShell 載入程式，最後會部署重度混淆的 DarkCloud 可執行檔。此行動強調反分析措施和規避策略。

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-Wscr!g1
- ACM.Rgasm-Lnch!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：

- ISB.Downloader!gen60
- ISB.Downloader!gen68
- ISB.Dropper!gen1
- Phish.ScptML.L
- Scr.Heuristic!gen22
- Scr.Malarchive!gen7
- Scr.Malcode!gdn32
- Scr.Malcode!gen
- Scr.Malcode!gen43
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- XSNet.Heur!gen3
- XSNet.Heur!gen11

- XSNet.Js!gen1
- XSNet.Ps1!gen2
- XSNet.Xml!gen1
- Web.Reputation.1
- Web.Reputation.3
- 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!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。

2025/08/21

CORNFLAKE.V3後門程式透過「ClickFix」類型攻擊行動散播

研究人員發現一起全新攻擊行動，CORNFLAKE.V3 後門正涉入其中，威脅組織 UNC5518 使用複雜社交工程手法來假冒圖靈 (CAPTCHA) 驗證機制的頁面進行傳播。根據他們發現，該後門目前有 Node.js 和 PHP 兩個版本，兩者都能竊取系統資訊、傳送各種有效酬載，並透過 Windows 註冊表 Run 機碼來維持其持久性／常駐，使其比早期版本更為進階。Node.js 變種會安裝 Node.js，並注入 base64 編碼的後門，而 PHP 版本則會執行額外的植入程式，例如：WINDYTWIST.SEA。一旦入侵成功，攻擊者會執行 Active Directory 偵查，並使用 Kerberoasting 竊取憑證。

網路知識：ClickFix 為「複雜的社交工程手法」，偽裝成系統錯誤訊息或文件註冊提示，圖靈驗證等名義為誘餌，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。要求使用者點選特定按鈕，然後依照指示以快速鍵開啟執行視窗、貼上等操作來「修正」問題，但實際上，這麼做是將剛才暗中複製的惡意命令貼上並執行，使得駭客得以對受害電腦上下其手。

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：

- PHP.Backdoor.Trojan
- JS.Downloader
- Trojan Horse

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。

2025/08/21

UNC1151進階持續威脅(APT)組織在最新攻擊行動中運用啟用巨集的試算表與雲端C&C

UNC1151 進階持續威脅 (APT) 組織已被觀察到透過惡意壓縮檔進行針對烏克蘭和波蘭的惡意軟體攻擊行動，惡意壓縮檔包含內嵌混淆巨集的誘餌試算表。這些檔案透過網路釣魚電子郵件傳送，會觸發第一階段植入程式的下載與執行，該植入程式會收集系統資訊，並協助從 C&C 伺服器部署其他惡意軟體。該威脅者已進一步發展其工具包，將雲端託管的協作服務整合至 C&C 通訊，並重複使用先前行動中觀察到的基礎架構模式。

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.Exl-Cmd!g1
- ACM.Exl-CPE!g1
- ACM.Exl-Rd32!g1
- ACM.Exl-Wmic!g1
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MSExcel!g4
- SONAR.MSExcel!g6
- SONAR.MSExcel!g11
- SONAR.SuspLaunch!g263
- SONAR.SuspLaunch!g333
- SONAR.SuspLaunch!g316

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：

- Backdoor.Ratenjay
- ISB.Downloader!gen68

- ISB.Downloader!gen433
- ISB.Heuristic!gen10
- Trojan.Gen.MBT
- XSNet.Vba!gen2

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: Rundll32 Suspicious Network 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。

2025/08/21

聯網裝置成為DDOS攻擊的幫兇～新出現MountBot殭屍網路

研究人員最近報告一個全新的物聯網殭屍網路：MountBot，這是 4 月份首次觀察到的殭屍網路，它利用華碩 AiCloud 的漏洞，在與 RapperBot 相同的基礎架構上運作。為了逃避偵測，它會透過綁定掛載 /proc/1 來隱藏程序，同時也會停用沙箱工具、對手惡意軟體，甚至是一般下載指令。該惡意軟體有多種變種，包括利用 CVE-2021-36260 的 Hikvision 裝置掃描器，並透過使用 iptables 阻擋外部存取，進一步確保安全性被控制。其掃描器可透過標示 User-Agent: Hello-World/1.0 的 GET 請求來識別，GreyNoise 也追蹤到這種模式。最近幾週的命令與控制流量顯示，大部分 DDoS 攻擊都以中國為目標，不過日本伺服器 (尤其是 Minecraft 伺服器) 也受到影響。

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：

- Linux.Mirai

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：

- Attack: Hikvision Command Injection CVE-2021-36260

2025/08/20

養成好習慣～下載(安裝／更新)程式務必從原廠網站：假冒Flash更新程式，散播Winos木馬程式

我們發現到一種偽裝成 Flash 外掛程式更新的新型 Silver Fox 攻擊行動。使用者會被偽造的線上工具 (例如：偽造的翻譯網站) 誘騙，他們會被提示安裝詐騙性的 Flash 更新。一旦執行，惡意軟體會安裝惡意載入程式，然後設定持久性／常駐能力、擷取其他元件並最終部署 Winos 木馬程式。此木馬程式允許攻擊者擷取螢幕截圖、記錄鍵盤按鍵並竊取剪貼簿資料，讓攻擊者能夠取得遭入侵電腦很高的權限。該攻擊行動顯示 Silver Fox 持續依賴社交工程、混淆和假冒軟體安裝程式，以達到隱匿和長期入侵的目的。。

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

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。

2025/08/20

EncryptHub駭客組織利用MMC CVE-2025-26633漏洞傳送有效酬載

最近，駭客組織 EncryptHub(又名 LARVA-208 和 Water Gamayun) 結合社交工程與微軟管理主控台 (MMC) 漏洞的攻擊行動，該漏洞被常見漏洞與暴露 (CVE) 編號為 CVE-2025-26633，稱為 MSC EvilTwin。該攻擊行動透過冒充 IT 支援、透過 Microsoft Teams 啟動遠端會話，以及利用 PowerShell 指令碼部署惡意 .msc 檔案來攻擊目標組織。攻擊鏈包括一個 PowerShell 惡意程式載入器，它會注入兩個 .msc 檔案：一個良性檔案和一個惡意檔案。惡意檔案被策略性地放置在特定目錄中，因此當執行合法的 .msc 檔案時，漏洞會允許 mmc.exe 載入並執行惡意的對應檔案，執行攻擊者的有效酬載。下一階段的有效酬載會滲出系統資訊、建立持久性，並從 C&C 伺服器解密 AES 加密指令，包括部署新增的資料竊取工具。

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：

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：

- ISB.Exploit!gen13
- Heur.AdvML.C
- Trojan Horse
- Trojan.Gen.2

- Trojan.Malscript
- Web.Reputation.2
- Web.Reputation.3
- WS.Malware.1
- WS.Malware.2
- XSNet.Ps1!gen1

基於機器學習的防禦技術：

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

2025/08/19
防護亮點：Google翻譯如何被濫用於網路釣魚行動

網路釣魚攻擊持續進化，變得更具欺騙性，也更難被使用者和安全工具偵測到。最近出現一種值得注意的手法：濫用 Google 翻譯來掩飾惡意網站。日文網路的釣魚行動有越來越多使用這種伎倆，利用使用者對翻譯服務和熟悉網域的信任。

透過將網路釣魚網頁包裝在 Google 翻譯框架中，攻擊者可以隱藏實際的目標網址，並使網站看起來合法。這在日本尤其有效，因為日本人對 Google 的信任度很高，而且語言障礙可能會掩蓋警告訊號。

此方法依賴 Google Translate 的網頁翻譯功能，可透過「translate[.] google[.]com」網域呈現任何公開網站。攻擊者在自己的基礎架構上建置網路釣魚網頁，並透過 Google 翻譯傳遞這些網址內容。

如何運作

- 釣魚電子郵件傳送--目標受害者會收到一封精心製作的釣魚電子郵件，冒充日本公司、政府機構或線上服務。
- 翻譯包裝的網址內容--網址內容並非直接連結至惡意網域，而是像這樣包裝：hxxps://translate[.]google[.]com/translate?hl=ja&sl=auto&u=hxxp://malicious*惡意的[.]example*某某[.]com
- 使用者感知--受害者看到頂部的 Google 翻譯工具列和一個「已翻譯」的釣魚網頁。瀏覽器顯示「translate[.]google[.]com」，這是一個可信賴的網域。
- 憑證竊取--釣魚網頁會擷取憑證、付款詳細資料或其他敏感資訊。

這種濫用可能會利用電子郵件和網頁安全的幾個盲點，例如：

- 混淆式網址(URL Obfuscation)--當 'translate[.]google[.]com' 被視為安全時，電子郵件過濾器可能偵測不到惡意網址，尤其是在檢查 'u=' 的參數時。此外，託管在雲端 buckets 上的釣魚網頁可以附加到 'translate[.]goog'。

- 網域信任--使用者信任 Google 網域上託管的連結。
- 預覽限制--電子郵件預覽或懸停工具提示通常只顯示主網域。
- 偵測能力降低--由於頂級網域看似合法，某些威脅情報系統可能不會將翻譯後的頁面標示為可疑。

網路釣魚工具包也越來越多根據地理位置和語言設定來量身打造內容，使得日語攻擊對當地目標更具說服力。

範例：假冒 Amazon 的日本語釣魚行動

這封釣魚電子郵件經過精心製作，看起來像是合法的 日本 Amazon 寄出的付款失敗通知，說明 600 日圓的 Amazon Prime 訂閱付款無法處理，並要求收件人更新其付款方式。寄件者位址被偽造，看起來像是來自 Amazon，但內嵌的連結卻揭露真正的用意。它並未指向 Amazon 網域，而是使用 translate.goog 網址 (即 Google 翻譯的網頁翻譯服務) 來重導向至釣魚頁面。

這種手法在全球都被觀察到 (過去幾個月來有數百萬封惡意電子郵件被封鎖)，但日本是經歷多次攻擊活動且持續成為攻擊目標的地區之一。以下是一些與最近在日本看到的活動相關的電子郵件主題範例：

- 【連続エラー通知】決済処理が複数回失敗しています｜アカウントがロックされる可能性があります
- 【アマゾン】アカウントなお知らせ（ メール番号:LJTBAFL-474239254
- 【アマゾン】アカウントの情報更新をお届けします!
- ＜緊急!エポスカード 重要なお知らせ＞

- 【エポスカード】お支払い金額確定のご案内
- 【エポスカード】お客様のアカウント認証に関するお知らせ
- 【エポスカード】二段階認証の導入についてのお知らせ
- 【エポスカード】本人情報緊急確認
- 【エポスカード】重要:必ずお読みください
- 【エポスカード】個人情報確認
- 【重要なお知らせ】お客様のお支払い方法が承認されません
- 【アマゾン】安全なアカウント利用のため、情報更新をお願いします
- 【アマゾン】承認手続きのお願い
- 【JAネットバンク】【重要】お客様の口座が凍結されました
- 【緊急情報】お客さま情報・取引目的の確認
- 【緊急】JAネットバンク お取引を保留した（必ずご確認ください）
- 【JA バンク】お客様情報・取引目的等のご確認
- 【JAネットバンク】利用停止のお知らせ
- 口座所有権の証明（名前、その他個人情報）
- 【緊急】【重要】取引を規制いたしました
- 【農業協同組合】振込（出金）、ＡＴＭのご利用（出金）利用停止のお知らせ

註解：對照日文的翻譯如下:

＊[連續錯誤通知] 付款處理多次失敗｜您的帳號可能會被鎖定
＊[亞馬遜] 帳戶資訊通知 (電子郵件號碼: LJTBAFL-474239254)
＊Amazon.com：您的帳號資訊已更新！
＊緊急！Epos卡重要通知
＊[Epos Card] 付款金額確定通知
＊[Epos Card] 有關客戶賬戶核實的通知
＊[Epos Card] 關於引入兩步驗證的通知
＊[Epos Card] 緊急確認身份資料
＊[Epos Card] 重要提示：請仔細閱讀
＊[Epos Card] 確認個人資料
＊[重要通知] 您的付款方式未被認可
＊[亞馬遜] 請更新您的資料以安全使用帳戶
＊[Amazon] 請求核准程序
＊[JA Net Bank] [重要通知] 您的帳戶已被凍結
＊[緊急資訊] 確認客戶資料和交易目的
＊[緊急資訊] JA Net Bank交易已被暫停 (請務必確認)
＊[JA銀行] 客戶資料、交易目的等的確認
＊[JA Net Bank] 暫停使用
＊帳戶所有權證明（姓名、其他個人資料）
＊[緊急] [重要] 交易已被限制
＊[農業合作社] 暫停轉帳（提款）、暫停使用 ATM（提款）的通知

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。

2025/08/19

免錢的永遠最貴～破解版遊戲暗藏Lumma惡意竊密程式和SectopRAT遠端存取木馬

一個多階段的惡意軟體攻擊行動已被揭露，搜尋破解版遊戲的使用者會被誘騙下載安裝程式，先部署 Lumma 惡意竊密程式，然後再安裝 SectopRAT 遠端存取木馬。根據 Unit 42 研究人員指出，感染鏈嚴重依賴 AutoIt3.exe 這個免費的 Windows GUI 自動化工具，Lumma 和 SectopRAT 安裝程式都綁定了該副本，以執行有效酬載並維持持久性。為了逃避偵測，攻擊者使用混淆的批次腳本、.cab 檔案和誤導性的副檔名。Lumma 惡意竊密程式一開始會滲透憑證和敏感資料，之後 SectopRAT 會透過 AutoIt 的持久性載入器建立遠端存取，並與攻擊者的 C&C 基礎架構進行通訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rgasm!g1
- ACM.Rgasm-Lnch!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g221
- SONAR.SuspLaunch!g444

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.NSISHeur!gen2
- Trojan.Gen.NPE
- 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。

2025/08/19

模組化的PipeMagic後門程式偽裝成ChatGPT應用程式，瞞天過海

最近，一個以財務利益為動機的駭客組織利用 ChatGPT 桌面應用程式為幌子的掩飾下，最終部署模組化的 PipeMagic 惡意軟體。發現到的網路惡意行動與 CVE-2025-29824 漏洞的開採濫用有關，CVE-2025-29824 是 Windows Common Log File System 中的權限提升漏洞。開放原始碼的

ChatGPT 桌面應用程式是攻擊鏈執行的第一階段。它負責將內嵌的 PipeMagic 有效酬載直接啟動到記憶體中。惡意程式會從 C&C 下載的模組會儲存於記憶體中，讓攻擊者能控制該惡意程式在遭入侵的系統上的行為。

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

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.Trojan
- Trojan Horse
- Trojan.Dropper
- Trojan.Gen.MBT
- 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。

2025/08/19

近期被揭露Adobe Experience Manager的漏洞 (CVE-2025-54253/CVE-2025-54254/CVE-2025-49533)

最近揭露三個影響 Adobe Experience Manager(AEM) 軟體解決方案的漏洞。這些漏洞的特徵與影響如下：

- CVE-2025-49533 是 FormServer 模組中的 Java 反序列化漏洞，可能讓未驗證的遠端程式碼執行 (RCE)。

- CVE-2025-54253 是由於 admin UI 模組中的驗證繞過所導致的錯誤配置漏洞。
- CVE-2025-54254 是 XXE (XML External Entity Reference) 漏洞，會影響處理 SOAP 認證的 Web 服務，導致未經授權的檔案系統存取。產品廠商已在受影響軟體的最新版本中修正這些漏洞。

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 Experience Manager CVE-2025-49533
- Web Attack: Adobe Experience Manager CVE-2025-54253
- Web Attack: Malicious XML External Entity Payload Upload

2025/08/18

遠端存取木馬程式njRAT偽裝成瀏覽器型態的Minecraft遊戲

由於 Minecraft 即將改編為電影，網路犯罪份子正利用這股熱潮，散佈瀏覽器型態的模仿遊戲，但實際上隱藏強大的遠端存取木馬程式 njRAT。惡意軟體一旦安裝，攻擊者就能完全控制受感染的系統，竊取憑證、監視網路攝影機和麥克風、記錄按鍵、竄改檔案和遠端 shell 執行。為了維持持久性，njRAT 會將自己加入系統啟動項目，而作為一種反分析措施，如果偵測到安全工具，它會試圖讓系統當機。此行動突顯流行文化活動如何被利用來增加惡意軟體的散佈，並誘使毫無戒心的使用者被入侵。

網路知識：《MINECRAFT麥塊電影》(英語：A Minecraft Movie) 是一部於 2025 年上映的美國奇幻冒險喜劇電影，改編自 Mojang Studios 的電子遊戲《Minecraft》。

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-FlPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.Ratenjay!gen1
- SONAR.Ratenjay!gen2
- SONAR.SuspBeh!gen22

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：

- MSIL.Trojan!gen2
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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：

- Audit: Ngrok Activity 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。

2025/08/18

偽裝成GiftFlipSoft APP的Android手機／行動裝置平台上的惡意軟體

一款複雜的 Android 手機／行動裝置平台上的銀行金融惡意軟體：Lazarus Stealer 最近浮出檯面，其偽裝成看似良性的 APP：GiftFlipSoft。此惡意軟體會移除其圖示，並將自己從最近的應用程式清單中排除，以保持隱藏性。一旦安裝後，惡意程式會提升權限，並可讀取、傳送及刪除簡訊內容 (包括OTP：一次性密碼)、持續監控應用程式使用情況，以及在特定俄羅斯銀行應 APP 上部署網路釣魚覆蓋畫面，以蒐集密碼、卡號及憑證等敏感資料。它持續執行背景服務，並透過 WebView 網址連結從其 C&C 伺服器動態載入釣魚內容，並與 C&C 通訊以滲透裝置中繼資料和簡訊內容，同時接收遠端指令。

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。

- AdLibrary:Generisk
- Android.Reputation.2

2025/08/15

NOVABLIGHT惡意程式服務(MaaS)類型的惡意竊密程式，鎖定加密錢包為目標

NOVABLIGHT 是一種複雜全新惡意軟體即服務 (MaaS) 的惡意竊密程式，利用 Telegram 和 Discord 來進行散佈和作業支援。它偽裝成「教育工具」，透過社交工程誘惑 (例如：經常以法文標題重新包裝的遊戲安裝程式偽裝影片) 悄悄散佈。執行時，NOVABLIGHT 會採用多階段管道，包含預檢機制和強大的迴避策略 (例如：初始化、注入應用程式、資料收集、剪貼簿劫持、透過多種管道外洩和清理)。此惡意軟體以憑證和加密錢包為攻擊目標。

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-Cscr!g1
- ACM.Ps-Net!g1
- ACM.Ps-Rd32!g1
- ACM.Wscr!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.Gen
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.eputation.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。

2025/08/15

濫用近距離無線通訊(NFC)類型的PhantomCard手機／行動裝置平台惡意軟體

一個被稱為 PhantomCard 的近距離無線通訊 (NFC) 的新型惡意軟體已在真實網路情境上被發現，並正大肆針對 Android 銀行客戶進行攻擊。它的散佈鏈涉及偽裝成官方 Google Play 商店的網站，尤其針對巴西的使用者。惡意程式原始碼顯示，它可能源自於惡意程式即服務 (MaaS) 產品「NFU Pay」，該產品已在各種地下市場流通販售。PhantomCard 功能是依賴受攻擊裝置內建的 NFC 讀卡器來讀取受害者銀行卡資料，並將收集到的資訊傳回攻擊者。

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。

- AdLibrary:Generisk
- Android.Reputation.2

2025/08/15

Charon勒索軟體

Charon 是最近新發現的勒索軟體，利用 DLL 注入手法入侵目標電腦。此勒索軟體會加密使用者資料，並冠上 .Charon 副檔名。加密的技術上，Charon 採用混合加密模式，將 Curve25519 橢圓曲線加密技術與 ChaCha20 串流密碼整合在一起。贖金通知是一個名為「How To Restore Your Files.txt」的文字檔形式，並要求受害者聯絡攻擊者以取得進一步指示。Charon 具有刪除受感染機器上的備份檔案和卷冊陰影副本的功能，讓受害者無法從系統內建的備份機制還原。

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.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 Horse
- Trojan.Gen.2
- 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!100
- Heur.AdvML.B!200
- Heur.AdvML.C

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**。