保安資訊--本周(台灣時間2025/08/29)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 33 萬 8,900 台受保護端點上總共阻止了 5,520 萬次攻擊。這些攻擊中有 84.6% 在感染階段前就被有效阻止：**(2025/08/25)**

- 在**7萬9,700**台端點上，阻止了**2,310**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**6萬6,800**台端點上，阻止了**520**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬1,200**台**Windows**伺服主機上，阻止了**520**萬次攻擊。
- 在**5萬4,500**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**2萬200**台端點上，阻止了**120**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬8,800**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**7萬2,600**台端點上，阻止了**200**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,600**台端點上，阻止了**67萬5,000**次加密貨幣挖礦攻擊。
- 在**9萬1,700**台端點上，阻止了**790**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**539**台端點上，阻止了**7萬5,300**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 28 萬 5,100 個受保護端點上阻止了總計 1,300 萬次攻擊。**(2025/08/25)**

- 使用網頁信譽情資，在 **270.3K** 個端點上阻止 **11.7M** 次攻擊。
- 攔截 **40.7K** 個端點上 **1.2M** 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 **7.3K** 個端點上攔截 **172.4K** 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 **404** 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。

2025/08/28

駭客組織「Silver Fox」利用合法驅動程式的漏洞部署遠端存取木馬程式

Check Point 研究人員揭露一起由「Silver Fox」駭客組織所發起的攻擊行動，該行動利用微軟簽署的驅動程式 (amsdk.sys) 漏洞試圖在 Windows 10 及 11 系統上偷偷停用 EDR 與防毒防護機制。此手法為傳送 ValleyRAT 後門程式清除路障--該惡意程式源自 Gh0st RAT 後門程式，能在入侵後取得完整遠端存取、監控及持久化的操作能力。

Silver Fox 是長期活躍的中文威脅行為者，其活動主要集中於亞洲及鄰近地區，但攻擊行動亦已擴展至全球特定產業領域。

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.Rd32-CPE!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30
- SONAR.SuspLaunch!g266

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

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：

- System Infected: Trojan.Backdoor Activity 568

2025/08/28

手機助長詐騙，舉世皆然：假冒印尼退休金管理機構的惡意軟體攻擊正在撒網捕魚進行詐騙

一項可能與中國威脅者有關聯的針對手機行動裝置的複雜惡意軟體攻擊，正大肆鎖定印尼退休人員及公務員為目標，其手法是偽裝成國營退休基金機構「PT Dana Tabungan dan Asuransi Pegawai Negeri」(TASPEN)。初始攻擊是透過一個幾可亂真的釣魚網站展開，該網站採用流暢的印尼語呈現，並複製 TASPEN 官方品牌形象，誘使受害者下載安卓平台上的惡意 APP。該惡意軟體採用先進的規避技術，特別是 DPT-Shell 封裝技術，使其在靜態分析中隱藏惡意本質，僅在執行時才顯露危害能力。安裝後，它將作為全面監控工具運作。重要功能包括：SmsService 服務可攔截所有接收的簡訊，藉此竊取用於繞過雙重驗證及執行詐騙交易的重要一次性密碼 (OTP)。ScreenRecordService 則持續監控用戶操作，竊取銀行應用程式中輸入的敏感資料。在一個特別令人擔憂的發展中，CameraService 能夠錄製臉部影片，這不僅加劇身份詐騙的風險，更危及生物特徵安全措施的完整性。此外，該惡意軟體會收集聯絡簿資訊與通話紀錄，擴展其情報蒐集能力。與指令控制 (C&C) 伺服器的通訊透過加密 WebSockets 進行，既能實現即時資料竊取，亦可執行遠端指令。該惡意軟體更內建反分析功能，當遭遇安全分析工具時會主動偵測並停用自身運作，其極具威脅性不容小覷。

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。

2025/08/28

駭客集團：ShadowSilk正在鎖定亞洲政府機構發動混合語言的進階持續威脅(APT)攻擊

一份最近發布的報告詳述 ShadowSilk 駭客集團，該駭客集團採用混合語言 (中文與俄文) 運作，主要專注於從政府目標中竊取資料。該駭客集團在中亞與亞太地區活動頻繁，並與 YoroTrooper 駭客集團有很緊密的關係。該報告指出，由於基礎設施與工具集等因素，該組織與 YoroTrooper 存在顯著的重疊；然而證據顯示，ShadowSilk 因引入新發現到的基礎設施、戰術、技巧和程序 (TTPs) 及擴展攻擊目標，可以判定應該是一個獨立的實體。

初始入侵通常透過釣魚郵件引誘。一旦建立通道，ShadowSilk 便利用 Telegram 機器人作為指揮控制 (C&C) 的基礎架構，管理有效酬載下載、執行、資料竊取、更新等操作。攻擊者運用 Cobalt Strike 與 Metasploit 等漏洞利用框架，配合 Telegram 類型的惡意軟體發動攻擊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.Mimikatz!gen27
- SONAR.Powershell!g109
- SONAR.Powershell!g111
- SONAR.Stealer!gen1
- SONAR.SuspLaunch!g445
- 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：

- Backdoor.Trojan
- Hacktool.Mimikatz
- Hacktool.Revsocks
- Hacktool.SharpHound

- Trojan Horse
- Trojan.Gen.2
- 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
- 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
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 654

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。

2025/08/28

駭客組織SmartApeSG假冒圖靈(CAPTCHA)驗證機制部署NetSupport遠端存取工具及StealC v2

駭客組織 SmartApeSG 發動多階段攻擊鏈攻擊正利用遭到入侵的網站，注入偽造的驗證碼頁面，藉此誘騙使用者透過類似 ClickFix 的腳本執行隱藏指令。此舉將導致 NetSupport 遠端存取工具 (RAT) 被安裝以實現持久化／常駐及遠端控制，隨後部署 StealC v2 程式，進而從受感染主機竊取憑證與資料。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2

- ACM.Ps-Enc!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：

- Infostealer
- Trojan.Malmsi
- WS.Reputation.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: Suspicious Process Accessing Lets Encrypt Certified Site
- URL Reputation: 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。

2025/08/28

安卓平台上的知名木馬程式Hook，推出v3新版，擴增銀行金融的間諜軟體及勒索軟體的攻擊功能

一款新型的 Hook 安卓銀行木馬變種已現蹤，其傷害不止於憑證竊取，更透過全螢幕加密貨幣支付介面覆蓋進行勒索軟體詐騙。該木馬現支援 107 項遠端指令 (其中 38 項為新增功能)，能偽造 NFC 提示、支付介面覆蓋、鎖定畫面 PIN 碼竊取，並透過濫用 Android Accessibility 無障礙功能服務取得完全控制權。據信源自 ERMAC 變種的 Hook 同時具備間諜軟體功能，可進行螢幕串流、竊取簡訊、存取相機，並竊取加密貨幣錢包的恢復短語 (recovery phrase)。該惡意程式透過釣魚網站及 GitHub 等平台散佈的惡意的 .APK 獨立 APP 安裝檔，融合銀行木馬、間諜軟體與勒索軟體特性，構成全球性重大威脅。

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
- AppRisk:Generisk

2025/08/27
Cephalus勒索軟體

2025 年 8 月中旬，研究人員發現到兩起由「Cephalus」勒索軟體所涉入的資安事件。根據調查結果，攻擊者透過未啟用多因素驗證 (MFA) 的帳戶利用遠端桌面協定 (RDP) 來入侵系統，並在部署有效酬載前似乎透過 MEGA 雲端硬碟服務平台竊取數據。與傳統攻擊方式不同，Cephalus 透過濫用合法的 SentinelOne 可執行檔 SentinelBrowserNativeHost.exe 進行 DLL 側載，藉此載入惡意 DLL 及嵌入的勒索軟體程式碼。啟動後，該程式會刪除系統快照副本以阻斷復原途徑，並透過 PowerShell 指令與登錄檔操作嘗試從系統層面停用 Windows Defender 防護機制。加密檔案會被冠上 .sss 附檔名，並在多個位置放置勒索贖金支付說明文件檔 (recover.txt)。

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.SuspLaunch!g250
- SONAR.Cryptlocker!g42
- SONAR.Ransom!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.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/08/27
中國駭客組織UNC6384利用「PlugX」後門程式進行間諜和情報行動

名為 UNC6384 中國駭客組織正在發動複雜的網路間諜行動，並且大肆鎖定東南亞外交官及其他全球性機構。該行動具有多階段攻擊鏈的特色，精心設計的隱蔽與規避能力。該行動首先透過「中間人攻擊」(AitM) 技倆進行 captive portal 劫持，將受害者網路流量重導向至看似合法的 Adobe 外掛更新頁面。隨後下載含有數位簽章且被辨識為 STATICPLUGIN 的惡意程式下載器。該惡意程式下載器偽裝成常見的 Microsoft Visual C++Redistributable 套件安裝程式，其主要功能是擷取內含惡意軟體的 MSI 封裝檔為後續攻擊鏈所需。此 MSI 封裝檔中暗藏名為 CANONSTAGER 的惡意啟動程式，該元件運用進階混淆技術，包含自訂 API 雜湊運算與執行序局部儲存 (Thread Local Storage：TLS)。此外，它透過 Windows 訊息佇列與視窗程序執行間接程式碼，實現 RC4 加

密後門程式 SOGU.SEC(亦稱 PlugX) 的隱蔽執行。此後門程式完全在記憶體中運作。該攻擊行動透過使用有效程式碼簽署憑證，並採用加密記憶體載荷特性，大幅提升整體效能，阻礙安全解決方案的偵測能力非常強。

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
- Trojan.Gen.MBT
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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：

- Audit: MSIEXEC Process Accessing Lets Encrypt Certified Site
- System Infected: Meterpreter Reverse Shell Payload
- 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。

2025/08/27

ZipLine供應鏈網路釣魚行動：建立信任，利用信任--詐騙手法的底層邏輯

稱為「ZipLine」精心設計的社交工程攻擊行動，鎖定美國製造業、半導體業及生物科技等多個領域的企業，意圖竊取重要資料、供應商網路或可利用的基礎設施。與傳統網路釣魚不同，ZipLine 行動透過企業公開的「聯絡我們」表單建立初始聯繫，藉此營造合法性。攻擊者會進行多次的電子郵件往來，假扮潛在商業夥伴，甚至要求簽署保密協議以建立信任。其現行詐術

是利用「AI 轉型」作為幌子，將釣魚行動包裝成「AI 影響評估」，藉此徵求受害者對 AI 採用的意見。為提升可信度，攻擊者採用模仿合法美國有限責任公司 (LLC) 的網域名稱，常使用先前持有網域搭配相似的風格網站，顯示其高度組織化與可擴展的攻擊行動。感染鏈始於內藏惡意程式的 ZIP 壓縮檔，通常保存在 Herokuapp.com 等合法平台以規避偵測。該壓縮檔內含惡意 .lnk 捷徑檔，並混雜無害的 PDF 與 DOCX 文件。此 .lnk 檔案會啟動 PowerShell 載入程式，部署名為「MixShell」的自訂記憶體植入程式。MixShell 以隱蔽性為首要目標，採用 DNS TXT 通道技術建立指令與控制 (C&C) 通道，並具備 HTTP 備援機制。其功能涵蓋檔案操作、反向代理、指令執行及互動式會話。此植入程式運用多項進階技術，包括採用 ROR4 雜湊演算法解析 API、透過記憶體執行減少磁碟鑑識痕跡，以及混淆配置檔案。持續性則透過 TypeLib 劫持機制維持，而 MixShell 的 PowerShell 變種更整合強大的反偵錯與沙箱規避機制。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g*

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!gen*
- Scr.Malarchive!gen7
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.xSense.C
- WS.Malware.1
- WS.SecurityRisk.4
- XSNet.CL!gen2
- XSNet.Ps1!gen1

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。

2025/08/27

Datebug威脅組織利用自訂惡意軟體鎖定BOSS Linux系統

Datebug 威脅組織 (又稱 APT36、Transparent Tribe) 是隸屬於巴基斯坦的威脅組織，主要鎖定印度境內各產業 (政府、媒體、軍事機構) 發動攻擊。近期觀察發現，該組織正針對 BOSS Linux 作業系統部署客製化惡意軟體，尤其鎖定印度政府的相關系統。

此次攻擊是透過含有壓縮檔附件的惡意垃圾郵件發動。該壓縮檔內含一個負責後續行動的 .desktop 捷徑檔案，其功能包括：從攻擊者控制的伺服器下載、解碼並執行惡意有效酬載，同時

透過 Firefox 載入誘餌檔案以掩蓋活動痕跡。攻擊者利用此有效酬載與 C2 伺服器維持通訊，用於接收指令、竊取資料外洩，以及下載額外有效酬載。

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：

- Downloader.Trojan
- Linux.Trojan

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。

2025/08/26

冒用生物科技與半導體公司的Snake Keylogger惡意竊密軟體散播行動

賽門鐵克發現攻擊者發動了兩波互相配合的惡意垃圾郵件行動，冒用知名企業名義散佈「Snake Keylogger」惡意竊密軟體。此款常見的惡意竊密軟體專門收集憑證、詳細系統資訊及其他敏感資料，隨後將這些資訊傳輸至攻擊者控制的 Telegram 機器人。

首波攻擊行動偽裝成一家以先進療法研究聞名的生物科技公司。攻擊者假借付款通知之名發送電子郵件，誘使收件者開啟惡意附件。第二波攻擊則冒充全球半導體與製造解決方案供應商，將訊息偽裝成報價請求，誘使目標受害者執行惡意軟體。

觀察到的電子郵件主旨：

- AAV-CAG-HA-SOLO257 Payment *付款通知
- Request For Quotation *報價需求

兩次攻擊活動均遵循精簡的傳遞鏈：電子郵件→惡意附件 (RFQ.xlam)→漏洞利用→有效酬載安裝。該 XLAM 試算表檔案 (偽裝成合法商務文件) 利用 CVE-2017-11882 漏洞，從攻擊者基礎設施下載 Snake Keylogger 的二進位檔。

攻擊分析顯示，目標範圍廣泛涵蓋：

- 旅遊與酒店業 (英國)
- 媒體與新聞業 (英國及以色列)
- 保險與金融服務業 (英國、歐洲及全球)
- 教育機構 (阿曼)
- 製造業與工業企業 (埃及、塞爾維亞、土耳其)
- 慈善機構與政府服務 (英國)

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

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：

- Exp.CVE-2017-11882!g5
- MSIL.Packed.19
- Scr.Malcode!gdn34
- Trojan.SnakeKeylogger

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/08/26

防護亮點：運用賽門鐵克端點偵測與回應(EDR)防護技術阻斷長期埋伏的進階持續威脅(APT)與勒索軟體威脅

為了在受害者環境中長期維持立足點，攻擊者運用持久性／常駐技術--這類方法目的在確保即使系統重新開機、憑證變更或防禦行動發生，仍能維持不中斷的存取權限。透過具有持久性的能力，攻擊者得以延長其存活的時間，進而竊取資料、進行間諜活動，並在網路中橫向移動。

對攻擊者而言，持久性／常駐是貫穿整個入侵過程的基石戰術。對防禦者來說，偵測並清除這些企圖對於防止長期入侵非常重要。 持久性之所以重要，在於它能：

- 實現長期隱蔽存取
- 支援隱蔽的資料收集與間諜活動
- 增加偵測與應對的複雜性
- 促進環境內的橫向移動

已知常見的持久化技術

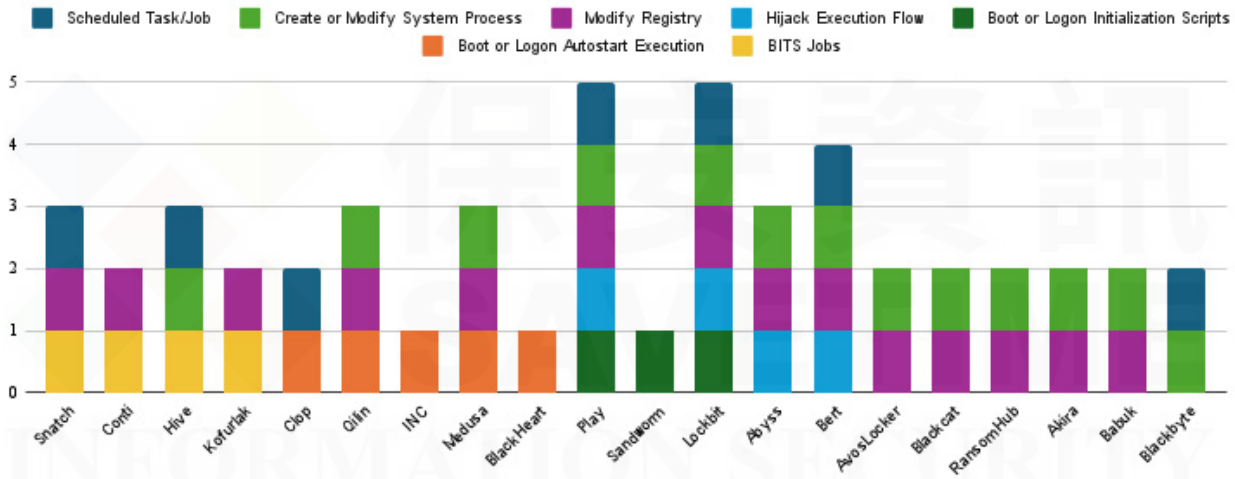
根據 MITRE ATT&CK 框架的威脅活動分析顯示，攻擊者反覆採用多種作業系統核心層級的持久化機制。在賽門鐵克客戶環境中，以下技術最為突出：

- 修改登錄檔 (T1112)：攻擊者竄改登錄檔機碼以保存有效酬載，或設定支援執行與持久化的指令。

- 啟動或登入自動執行 (T1547)：惡意二進位檔或腳本被設定在系統啟動或使用者登入時自動執行。
- 排程任務／工作 (T1053)：攻擊者建立排程工作，確保有效酬載在啟動時或指定間隔內重複執行。
- 劫持執行流程 (T1574)：
  - DLL 側載：利用合法應用程式載入攻擊者提供的 DLL 檔案。
  - DLL 搜尋順序劫持：利用 Windows 搜尋順序漏洞，使惡意 DLL 優先於合法檔案載入。
- 建立服務 (T1543)：建立自訂惡意服務以維持持久性，並混入正常系統運作中。。

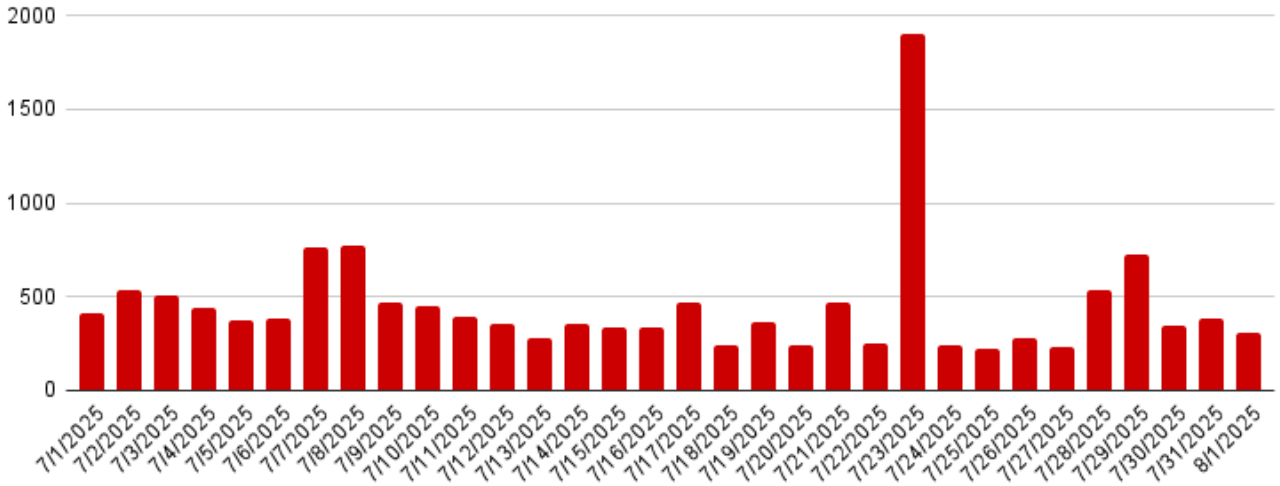
勒索軟體家族與持久性機制

持久性機制並非僅見於進階持續威脅 (APT) 攻擊--勒索軟體經營者同樣高度依賴這些技術。針對多個勒索軟體家族的分析顯示，它們傾向透過修改登錄檔、設定工作排程、劫持動態連結庫 (DLL) 及建立服務等方式來維持控制權。詳見以下概述：

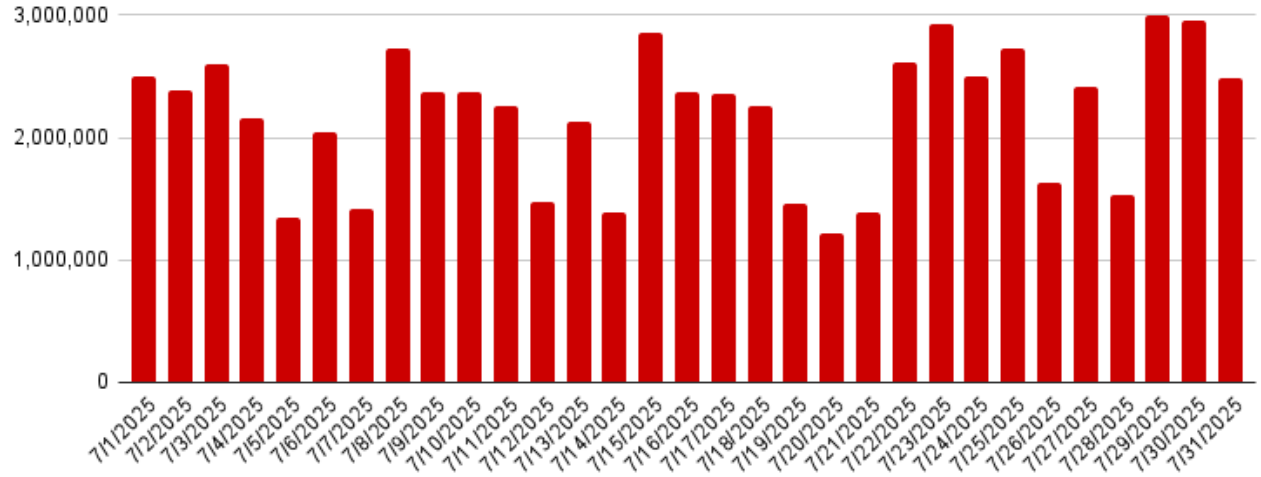


賽門鐵克 EDR 阻斷長期埋伏的持久化機制

賽門鐵克 EDR 阻斷長期埋伏的持久化相關活動，防止攻擊者將自身植入客戶環境。每日遙測資料顯示這些防禦措施的規模，如下所示：



除了封鎖攻擊外，EDR 還能深入洞察惡意程式持續存在的行為模式，賦予防禦者調查可疑活動的能力，將其與攻擊者戰術建立關聯，並在惡意程式擴散造成更嚴重損害前主動應對。賽門鐵克 EDR 每日偵測數百萬次惡意程式持續存在的企圖，如下圖所示。



持久性是攻擊者武器庫中最關鍵的戰術之一。從進階持續威脅 (APT) 組織到勒索軟體經營者，攻擊者皆仰賴登錄檔竄改、工作排程、DLL 劫持及惡意服務來確保長期存取權限。賽門鐵克 EDR 不僅能大規模阻斷此類企圖，更賦予防禦者深入調查與修復的可視性。

阻斷持久性就是瓦解攻擊者的控制權--這正是捍衛企業環境的關鍵決策步驟。

關於賽門鐵克EDR 的原廠官方網站介紹，請點擊此處。
欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

2025/08/26

免錢的永遠最貴～偽裝成防毒軟體的全新安卓平台上後門程式，專偷俄羅斯企業領袖的情報

一款全新且複雜的安卓平台手機行動裝置惡意軟體：Android.Backdoor.916.origin 已被發現，其鎖定目標為俄羅斯企業的高層主管。攻擊者採用詐騙的社交工程手法，透過熱門通訊平台私訊散佈偽裝成防毒軟體 APP「GuardCB」的惡意 .APK 獨立安裝檔案。該惡意軟體圖示擬真的仿造俄羅斯聯邦中央銀行標誌，進一步提升可信度並誤導潛在受害者。一旦安裝成功，Android.Backdoor.916.origin 便具備強大的監控能力：可主動監聽用戶對話、即時串流相機的即時串流影像，並透過內建鍵盤記錄器擷取所有按鍵操作。關鍵在於，該惡意軟體專門設計用於竊取大家普遍使用 APP(包括Telegram、WhatsApp、Gmail、Chrome及Yandex) 中的敏感通訊資料。為躲避偵測與移除，該惡意軟體採用精密偽裝手法：假冒防毒掃描。當用戶嘗試啟動掃描時，APP 會顯示預先設計好的模擬介面，謊報已偵測到少量的病毒結果，藉此延緩用戶的警覺並阻止即時卸載。此目標式攻擊手法結合多重惡意功能，對被鎖定的受害者隱私與安全構成重大威脅。

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。

- AppRisk:Generisk
- 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。

2025/08/26

Anatsa--安卓平台手機行動裝置的惡意軟體

Anatsa 是一款安卓平台手機行動裝置的銀行金融木馬程式，自 2020 年起便持續四處流竄。近期發現到的攻擊行動顯示，該惡意軟體是透過從 Google Play 商店的文件閱讀 APP 下載。近期版本具備以下功能：

- 反分析 (變更 APK 特性、運行時解密、隱藏有效酬載)
- 憑證竊取 (可能導致財務損失)
- 鍵盤記錄

Anatsa 鎖定數百款銀行 APP，意圖竊取用戶憑證。該惡意軟體會根據受害裝置上安裝的金融 APP，顯示偽造的登入頁面。

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

2025/08/26

Gayfemboy惡意軟體濫用常見無線分享器漏洞所發動的攻擊行動

一款名為「Gayfemboy」的隱蔽型惡意軟體，已被發現到濫用多種漏洞滲透系統。近期攻擊主要鎖定 DrayTek、TP-Link、Raisecom 及 Cisco 等廠商產品的漏洞。該惡意軟體影響範圍遍及全球，波及巴西、法國、德國、以色列、墨西哥、美國、瑞士及越南等國，並衝擊建築、製造、科技及媒體／通訊等產業領域。Gayfemboy 採用複雜的規避技術，包括：透過自訂檔案名稱規避可預測模式、使用修改版的 UPX 標頭進行混淆，以及建置自我保護機制。其核心模組包含：反分析監控與持久化功能、確保單一執行個體運作的看門狗機制、DDoS 攻擊與後門功能，以及用於清除競爭惡意軟體或強制自我終止的殺手模組。

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
- Linux.Mirai
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.NPE
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3

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。

2025/08/25

安裝APP請從安全的來源：Gigabud惡意軟體在東南亞偽裝成Grab Superapp

最近發現安卓平台上行動惡意軟體：Gigabud，冒充廣受歡迎的 GRAB Superapp(*超級應用程式)，提供乘車、點餐和數位支付服務，在東南亞各地廣泛使用。在泰國偵測到的特洛伊木馬安裝檔 .APK 檔名為 Grab.apk，偽裝成合法的 APP。

網路知識：Grab Holdings Inc.(NASDAQ：GRAB) 為東南亞軟體平台巨頭，於 2012 年在馬來西亞創立。Grab 初期以快速模仿對手並強砸補貼進入市場，後期的營運開始逐漸發揮本地化的優勢，形成自己的特色，甚至在 2018 年併購 Uber 的東南亞業務，自此奠定下其東南亞叫車平台霸主的地位。雖然 Grab 是以叫車服務起家，但其所提供的服務還包含外送及金融服務等。Grab 將自己定位為東南亞首屈一指的 Superapp，基於叫車、外送、金融服務業務輻射到生活中的各個角落，業務邊界的拓展也是近幾年迅速擴張的重要原因。「Superapp」指的是在同一個 App 中提供多樣化的服務，這些服務甚至不歸屬於同個類別，使消費者不用離開 App，就能夠在同個 App 內使用所有的服務，除了方便性外，也有利於企業建立屬於自己的生態系。Grab 從一開始的叫車平台，逐漸發展成整個東南亞的全方位 Superapp，提供服務橫跨叫車、美食及生鮮外送、金融服務，例如：支付解決方案等。Grab 想成為「The Everyday, Everything Superapp」的願景不僅透過服務多元化達成，其在東南亞各國的在地化也十分成功，例如：摩托車叫車服務，在許多交通堵塞的地區十分受歡迎。(知識來源：https://www.forecastock.tw)

一旦安裝，假冒的 APP 會呈現極為相像 GRAB 品牌介面。截圖顯示登入畫面與真正的服務如出一轍，並有 GRAB 標誌和配色方案，目的是讓使用者相信其真實性。然而，在光鮮的外表下，Gigabud 立即提示存取服務的權限，使其能夠監控活動、竊取憑證，並可能繞過雙重認證。

儘管確切散佈途徑尚未證實，但早期證據顯示是手機簡訊釣魚，這是 Gigabud 網路犯罪份子先前使用的方法。受害者會被誘騙透過冒充可信賴品牌連結下載惡意 .APK 的 APP 獨立安裝檔。

Gigabud 曾針對銀行、加密貨幣平台和政府服務進行螢幕錄製、憑證竊取和金融詐騙。其最新冒充 GRAB 的行為，突顯出該網路犯罪組織濫用可信的日常 APP 來擴大感染範圍，並加深其在東南亞的足跡的策略。

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：

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。

- AppRisk:Generisk

2025/08/25

Sinobi 勒索軟體正在危害全球

Sinobi 勒索軟體的勒索贖金說明使用標準之雙重勒索手法。它混合恐嚇 (被盜文件、7 天期限、洩密威脅) 與說服 (測試解密和被盜文件清單)。勒索贖金說明 (README.txt) 提供多個 Tor 加密連結以供協商，並提供唯一的受害者 ID。成功入侵並加密後，遭加密的檔案會冠上 .SINOBI 副檔名。

拆解Sinobi 勒索軟體的戰術、手段、流程(TTPs)，顯示廣泛使用 ATT&CK 矩陣中已歸類的伎倆，與現代的雙重勒索攻擊手法相符。

- 初始存取 (TA0001)--透過可攜式媒體複製 (T1091)
- 執行 (TA0002)--指令和腳本編譯器 (T1059)；共用模組 (T1129)
- 持久性 (TA0003)--建立或修改系統程序：Windows 服務 (T1543.003)
- 權限提升 (TA0004)--存取權杖操控 (T1134)；濫用權限提升控制機制 (T1548)
- 防禦規避 (TA0005)--混淆/加密檔案 (T1027)、軟體封裝 (T1027.002)、偽裝 (T1036)、指示符移除 (T1070)、解除混淆/解碼檔案 (T1140)、檔案權限修改 (T1222)
- 憑證存取(TA0006)--作業系統憑證傾印 (T1003)、不安全的憑證 (T1552)、檔案中的憑證 (T1552.001)
- 搜索 (TA0007)--系統服務搜索 (T1007)、查詢機碼 (T1012)、程序搜索 (T1057)、系統資訊搜索 (T1082)、檔案與目錄搜索 (T1083)、週邊裝置搜索 (T1120)、網路共用搜索 (T1135)、軟體搜索 (T1518)
- 收集 (TA0009)--本機系統資料 (T1005)、暫存資料 (T1074)、螢幕擷取 (T1113)、電子郵件收集 (T1114)
- 指揮與控制 (TA0011)--透過 Tor 的代理 (T1090)
- 影響 (TA0040)--資料銷毀 (T1485)、加密資料的影響 (T1486)、停止服務 (T1489)

受害者主要集中在美國，影響範圍包括製造商、工程公司、醫療保健、教育和安全服務。大多數聲稱的受害者似乎都是中型組織，而非大型企業，這反映出他們是隨機性的目標。

不只是美國，澳洲、台灣和新加坡也有受害者，顯示該集團進行全球佈局的野心。國際目標包括能源、電子及工業零組件產業。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransomware!g*
- SONAR.Ransom!gen98

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：

- Ransom.Lynx!gen1

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/08/25

Remcos遠端存取木馬(RAT)涉入的攻擊行動鎖定全球產業和政府機構

最近觀察到惡意垃圾郵件攻擊行動，是利用冒充閥門和致動器產業的全球供應商來傳送 Remcos 遠端存取木馬 (RAT)。此誘餌以電子郵件的形式出現，郵件主題為「Price quote」或「Quotation」，附件為惡意檔案 (Quote_pdf.z)。

這些電子郵件看起來很專業，有具名的員工、公司詳細聯絡資訊，以及連結到合法網站的連結，增加偽造的可信度。攻擊鏈遵循一個簡單但有效的順序：電子郵件→ZIP 壓縮檔→可執行有效酬載。

一旦受害者擷取並執行可執行檔 (Quote_pdf.exe)，就會安裝 Remcos 遠端存取木馬 (RAT)。此惡意軟體會賦予攻擊者遠端控制權，使憑證竊取、監視和進一步的惡意活動成為可能。

從受害者的網域顯示，此攻擊行動鎖定多個地區的廣泛產業，包括：

- 北美、歐洲和亞洲的金融和銀行業。
- 歐洲和亞太地區的能源、公用事業和建築公司。

- 美國、巴西和英國的政府機構和公共部門。
- 日本、德國和印度的科技、汽車和製造公司。
- 歐洲和中東地區的媒體、教育和研究機構。

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.SuspCreate!g12

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.Suspexec!gen8
- Packed.Generic.666
- Scr.Malcode!gdn34
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/08/25

不斷進化的APT36駭客組織以嶄新的傳輸技術嶄露頭角

APT36 駭客組織 (又稱 Transparent Tribe) 所發動新一起攻擊行動已經被報導，該攻擊行動利用含有偽裝成 PDF 惡意 .desktop 檔案的 ZIP 檔之網路釣魚電子郵件來攻擊使用者。這些檔案開啟後，會從 Google Drive 取得有效酬載、執入惡意程式並建立持久性，同時運用沙箱規避技術，最終提供攻擊者遠端存取權限。此行動反映 APT36 在採用非傳統傳送機制方面的持續進化，例如：Linux 桌面應用程式的啟動捷徑 (Desktop Entry)，以及濫用 Google Drive 等可信任平台以維持有效傳送與控制。

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：

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

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。

2025/08/25

哈薩克公共部門正遭受網路釣魚行動攻擊

在哈薩克發現一起網路釣魚行動，該惡意行動模仿政府官方入口網站，並使用 Telegram 的 Bot API 作為隱蔽管道，鎖定公共部門服務的用戶為目標，竊取他們的憑證。該攻擊採用預先填寫政府電子郵件欄位、偽造安全通知和視覺上令人信服的介面等欺騙手段，誘使使用者洩露資訊。惡意的 HTML 和 JavaScript 被用來攔截登入資料，並直接傳輸至攻擊者控制的 Telegram 聊天室，而某些變種也會將受害者重導向至合法的微軟支援頁面，以掩飾竊取的行為，並營造出幾可亂真的假象。

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：

- Phish.ScrHtml!gen6
- Web.Reputation.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。

2025/08/22

日本FamiPay使用者成為新型網路釣魚行動的目標

最近，賽門鐵克觀察到針對日本 FamiPay(FamilyMart 提供的日本數位錢包和行動支付服務)使用者的網路釣魚活動。FamilyMart 是日本主要的連鎖便利商店。威脅者最近發起偽裝成帳戶驗證電子郵件的網路釣魚活動。這些釣魚郵件試圖引誘受害者點擊包含的釣魚網址，並要求驗證帳戶資訊。這些電子郵件使用以下主旨：

- Subject:【重要】FamiPay 身分認証通知
- 翻譯：「[重要] FamiPay 身分認證通知」

點擊郵件中的鏈結後會將用戶重導向到一個竊取其憑證目的的偽造網頁。

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。

2025/08/22

SpyNote涉入的攻擊行動採用偽造IBM Trusteer行動APP

在持續監控的行動威脅期間，賽門鐵克發現一個偽裝成 IBM 安全產品的惡意安卓 APP。該 APP 以 IBMTMOBILE.apk 的檔名散佈，並託管在一個專門為 IBM Trusteer 設計的網域上。

IBM Trusteer 是一套合法的詐騙預防套件，以 Trusteer Rapport 最為人熟知，這是銀行用來保護客戶免受網路釣魚和金融惡意軟體侵害的瀏覽器外掛程式。在行動裝置方面，IBM 提供 Trusteer Mobile SDK，內嵌於官方銀行 APP 中，以偵測裝置被入侵與詐騙的風險。最重要的是，並沒有為消費者提供獨立的「IBM Trusteer Mobile」應用程式。

攻擊者可能會利用這種混淆，冒充銀行並鼓勵使用者安裝偽造 「Trusteer Mobile」 APK。誘餌通常會強調安全性或合規性--"install this app to keep banking safe" (安裝此應用程式以保證銀行安全) 或 "your account may be blocked without it."(沒有此應用程式，您的帳戶可能會被封鎖)。實際上，這種手法將保護變成入侵，以安全為幌子傳送惡意軟體。

該惡意應用程式可能是透過網路釣魚電子郵件、簡訊釣魚，或詐騙性的銀行提示散佈，經證實是 SpyNote，一種知名的 Android 遠端存取木馬程式 (RAT)，能夠擷取資料、錄製音訊、攔截訊息，並讓攻擊者完全控制受感染的裝置。

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。WebPulse 已知道此次活動中使用假冒的域名。

- 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。

2025/08/22

TA-NATALSTATUS加密劫持行動

TA-NATALSTATUS 是一個在全球各地從事加密劫持作業的威脅執行者。攻擊者針對易受攻擊的 Redis 伺服器裝置部署加密惡意軟體。據觀察，該組織利用多種技術協助他們保持相對低調，其中包括：時間壓縮技術、持久性、進程劫持、混淆等。

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2025/08/22

SharePoint ToolShell漏洞(CVE-2025-53770)被Warlock勒索軟體濫用發動全面性的網路攻擊

Warlock 勒索軟體威脅份子開採濫用存在 Microsoft SharePoint 中的嚴重等級漏洞 (CVE-2025-53770)，即近期很熱門的 ToolShell 漏洞利用鏈，大肆針對全球組織發動攻擊。Warlock 背後的威脅份子濫用此漏洞迅速攻陷未修補的系統，並運用一連串複雜的後期攻擊技術。該攻擊鏈針對 SharePoint 內的驗證和反序列化缺陷，讓攻擊者可以快速執行程式碼，並透過建立新的群組政策物件 (GPO)，以及賦予內建的「guest」帳戶管理權限來提升權限。然後，攻擊者會建立隱密的命

令與控制 (C&C) 通道，以逃避偵測，並使用標準的 Windows 工具 (例如：Command Shell) 來執行腳本和批次作業。這可讓攻擊者在遭入侵的網路中橫向移動，並大規模部署具破壞性的勒索軟體，目的是加密檔案，並留下勒索贖金支付說明。

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：

- AGR.Terminate!g2
- SONAR.Ransomware!g19
- SONAR.Ransomware!g30
- SONAR.Ransomware!g39
- 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：

- Ransom.Gen
- Ransom.Warlock!gen1
- 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
- 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。

2025/08/22

BQTLOCK勒索軟體

BQTLOCK 是一款以加密勒索即服務 (Ransomware-as-a-Service：Raas) 模式提供銷售的新型勒索軟體。該惡意軟體具有加密使用者資料的功能，並會冠上 .bqtlock 副檔名。這個勒索軟體背後的攻擊者還運用雙重勒索技術，威脅受害者如果不滿足贖金要求，就會公開暴露收集的資料。BQTLOCK 具備停用本機備份、系統復原和刪除遭入侵端點的卷冊陰影複本的功能。根據 K7 Security Labs 報告，最近發現新變種具有竊取憑證功能、增強的反分析能力、UAC 繞過功能和更強的混淆機制。

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-Schtsk!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- AGR.Terminate!g5
- AGR.Terminate!g7
- SONAR.SuspStart!gen2
- SONAR.SuspStart!gen10
- SONAR.SuspStart!gen13
- SONAR.SuspStart!gen14
- SONAR.SuspStart!gen15

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
- 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

2025/08/22

SHAMOS平台出現：源於AMOS的SHAMOS惡意軟體

SHAMOS 是針對 macOS 平台的 AMOS(也稱為 Atomic macOS 惡意竊密程式) 惡意軟體的新變種。此惡意軟體由 Cookie Spider 威脅組織以 MaaS(惡意軟體即服務) 的形式銷售。SHAMOS 最近透過惡意廣告行動散佈，利用假冒 macOS 技術協助網站引誘毫無戒心的使用者。已執行的惡意有效酬載具有資訊竊取功能，以及下載其他任意模組和元件的功能。

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：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- 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。

2025/08/22

QuirkyLoader：隱匿性更強的新型惡意軟體載入器

一個新發現惡意軟體載入器：QuirkyLoader 已經構成複雜的網路威脅，大肆散布一系列惡意竊密程式和遠端存取木馬 (RAT)，包括 Agent Tesla、AsyncRAT、FormBook、MassLogger、Remcos 等。最近攻擊行動特別針對台灣和墨西哥的企業，透過垃圾郵件傳送惡意檔案附件。QuirkyLoader 包裝一個合法的可執行檔，一個加密隱藏有效酬載和一個惡意程式載入器來啟動感染。一旦執行，它會利用 DLL 側載和合法 Windows 程序內的程序空洞化來隱匿部署其最終有效酬載。該載入器還採用一些技倆，以躲避傳統的 .NET runtime 檢測，使分析變得複雜，並使用加密混淆來進一步隱藏惡意活動。

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。

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.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。

2025/08/22

他山之石，可以攻錯～印度正流行假冒電力補貼的手機App釣魚行動

冒充印度政府電力補貼計劃的安卓手機平台之網路釣魚行動已被發現。受害者透過 YouTube 和 GitHub 架設的仿冒官方補貼入口網站釣魚。受騙後，他們會被誘騙下載並安裝惡意 .APK 的 APP 安裝檔，竊取統一付款介面 (UPI：Unified Payments Interface) 認證、簡訊內容訊息和聯絡資料，同時還能透過 Firebase 進行遠端控制。

網路知識：

- 統一付款介面 (UPI)：統一付款介面 (UPI) 是印度的即時付款系統，可以用來付款和在銀行帳戶之間轉帳。
- Firebase 是一個由 Google 提供的雲端平台，專為行動和網頁應用程式開發者設計，提供一系列緊密整合的後端服務，例如：資料庫、身份驗證、檔案儲存、應用程式分析和託管等功能，讓開發者無需管理伺服器，就能快速開發和擴充應用程式。

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：

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。

- AppRisk:Generisk
- Android.Reputation.2

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**。