保安資訊--本周(台灣時間2025/01/31)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 6,900 台受保護端點上總共阻止了 4,620 萬次攻擊。這些攻擊中有 81% 在感染階段前就被有效阻止：**(2025/01/27)**

- 在**7萬9,800**台端點上，阻止了**1,610萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬8,300**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**2萬4,700**台**Windows**伺服主機上，阻止了**6萬**次攻擊。
- 在**4萬9,600**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**85萬4,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,100**台端點上，阻止了**230萬**次嘗試利用的應用程式漏洞。
- 在**10萬4,900**台端點上，阻止了**220萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,500**台端點上，阻止了**99萬5,600**次加密貨幣挖礦攻擊。
- 在**10萬6,400**台端點上，阻止了**790萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**461**台端點上，阻止了**7萬9,400**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 16 萬 3,600 個受保護端點上阻止了總計 700 萬次攻擊。**(2025/01/27)**

- 使用網頁信譽情資，在 **156.9K** 個端點上阻止 **650** 萬次攻擊。
- 攔截 **17.8K** 個端點上 **291.5K** 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 **7.2K** 個端點上攔截 **143.7K** 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 **169** 個端點上攔截 **5.6K** 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。

2025/01/31

SparkRAT--跨平台的模組化惡意軟體

SparkRAT 是採用 Golang 撰寫的模組化惡意軟體家族，最初發現於 2022 年。SparkRAT 支援跨平台，可針對 Windows、macOS 和 Linux 等各種架構。就在去年，該惡意軟體涉入多起目標式網路間諜行動。過去，它也曾在濫用 JetBrains TeamCity 驗證繞過漏洞 (CVE-2024-27198) 的行動中遭散播。SparkRAT 使用 WebSocket 通訊協定和 HTTP 請求與攻擊者 C&C 伺服器通訊。分析攻擊者所使用的網路基礎架構，顯示攻擊者更針對在 macOS 上散佈此惡意軟體家族的後繼新變種，以及嘗試透過偽裝為線上遊戲平台的網站散佈惡意 Android APP 安裝套件。

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.Sparkrat!g1
- Trojan Horse
- Trojan.Gen.MBT
- WS.SecurityRisk.4

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

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: JetBrains TeamCity Authentication Bypass CVE-2024-27198

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。

2025/01/31

Windows Locker勒索軟體

在真實網路情境裡發現到 Windows Locker 勒索軟體家族的後繼新變種。此惡意軟體會加密使用者資料，並在被加密後的檔案冠上 .winlocker 的副檔名。勒索 (贖金支付) 說明存在隨附的「Readme.txt」的文字檔，內容包含如何與威脅者聯絡以及如何支付贖金請求的資訊。Windows Locker 勒索軟體的功能包括維持持久性／常駐能力、停用防火牆和工作管理員，以及刪除受攻擊機器上的備份和陰影複本。

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.HiddenTear!g1
- Ransom.Slam
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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。

2025/01/29

Aquabot v3--源於Mirai惡意軟體的後繼新變種

在真實網路情境裡發現到一個源於 Mirai 惡意軟體的後繼新變種，稱為 Aquabot v3。據報導，該惡意軟體開採濫用 CVE-2024-41710 這個影響各種 Mitel 裝置的指令注入漏洞。此惡意軟體也能利用一些影響 Hadoop YARN 或各種 Linksys 裝置的陳年老舊漏洞。Aquabot v3 支援多種架構，包括 x86 和 ARM。從功能上來看，該惡意軟體主要用於從遭駭入的設備發動 DDoS 攻擊。

賽門鐵克已經於第一時間提供多種有效保護(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.2
- 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：

- Attack: LB Link Command Injection Vulnerability CVE-2023-26801
- Web Attack: Gpon Router Cmd Injection CVE-2018-10561
- Web Attack: Gpon Router Cmd Injection CVE-2018-10562

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。

2025/01/29

GamaCopy駭客組織最近活動有增多的趨勢

據報導，GamaCopy 威脅組織在真實網路情境裡發動新一波的網路惡意活動。該駭客組織所使用的戰術、技巧和程序 (TTPs) 與另一個威脅組織：Core Werewolf 有一定程度的重疊，也仿效 Shuckworm (也稱為 Gamaredon) 威脅組織之前所進行的一些舊式攻擊。攻擊者利用自我解壓縮 (SFX) 檔案來傳送偽造的 .PDF 文件，以及用於遠端存取遭入侵端點的 UltraVNC 遠端桌面工具。

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：

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

基於機器學習的防禦技術：

- 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。

2025/01/29

TorNet後門程式

TorNet 是一款後起之秀的後門程式，在持續進行的惡意攻擊行動中經常被散播，主要針對德國和波蘭。發動攻擊的威脅份子也散佈其他各種惡意軟體有效酬載，包括 Agent Tesla 和 Snake Keylogger。根據思科 (Cisco) 旗下威脅情報組織 Talos 最近的報告，攻擊鏈利用偽裝成金融機構和製造業或物流業公司信件的網路釣魚電子郵件。這些電子郵件包含惡意 .tgz 壓縮檔附件，一旦解壓縮就會執行基於 .NET 惡意程式載入器的可執行檔，並呼叫 PureCrypter 惡意軟體。PureCrypter 功能是注入惡意的有效酬載。TorNet 後門有能力接收攻擊者的指令，並在受感染的機器上執行任意的 .NET 程式集。

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：

- Downloader
- MSIL.Downloader!gen8

- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.1
- 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
- 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
- System Infected: Trojan.Backdoor Activity 721
- 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。

2025/01/28

防護亮點：賽門鐵克靜態資料掃描技術(Symantec Static Data Scanner：SDS)的進階影像掃描技術如何搶先一步獲得QR code釣魚攻擊的預警來保護我們客戶

QR code 型態的網路釣魚攻擊多年來一直是持續的威脅，而且手法與技術日益複雜且精密。由於 QR code 現在被廣泛用來分享資訊，惡意行為者視其為不可多得的網路釣魚媒介與手法。近幾個月來，QR code 網路釣魚攻擊的規模和複雜性大幅增加。不幸是，傳統安全措施往往難以辨識惡意 QR code，尤其是當攻擊者運用創意與巧思來掩蓋其真正目的時。

為了因應這些挑戰，賽門鐵克開發並持續優化進階的影像掃描引擎，其只是賽門鐵克靜態資料掃描技術的一部分。此尖端解決方案專門用於識別和阻擋即使是最進階的 QR code 釣魚企圖。與傳統系統不同的是，它在複雜性或操控性可能會導致偵測失敗的情況下，仍能發揮出色的效能。以下是讓我們的引擎與眾不同的幾項主要功能：

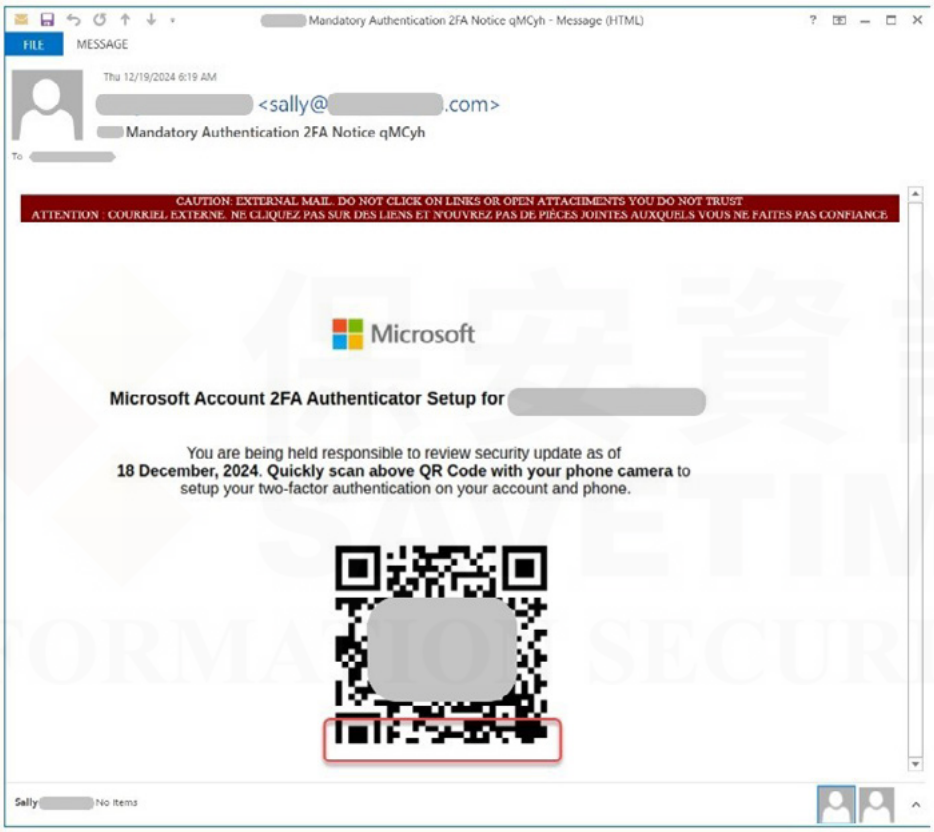
- **全面的格式支援**：無論 QR code 是嵌入在 PDF 或 Word 文件中，我們的引擎都能有效掃描和處理。
- **高度容錯性**：我們的技術可以準確偵測到模糊、損壞、截斷或具有不規則配色方案和形狀的 QR code
- **可擴充性與效能**：引擎對於不同尺寸的 QR code，從微小的角落標誌到大型設計，都有同

樣優異的表現

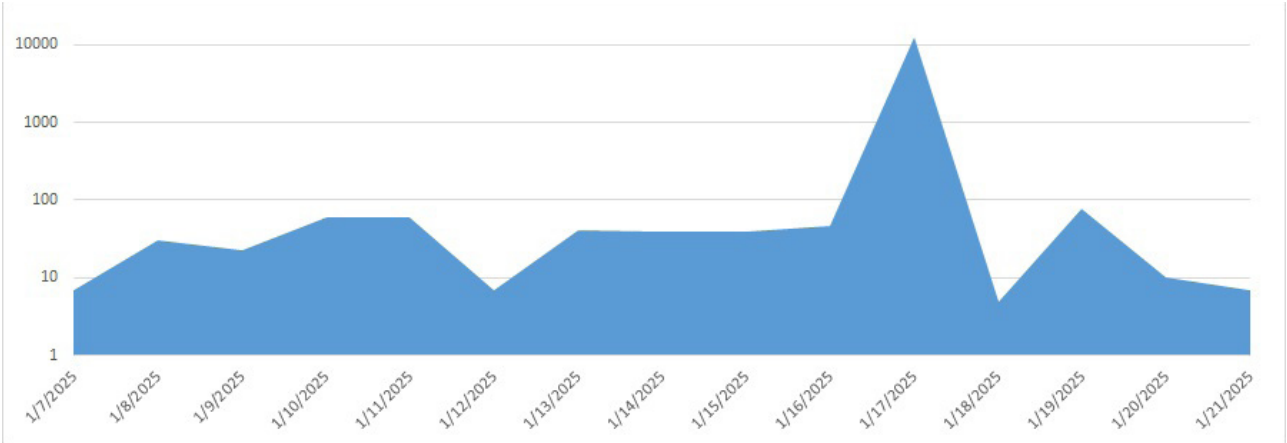
- **AI 驅動偵測**：利用進階的演算法，引擎可以識別和解碼故意設計來繞過傳統掃描工具的 QR code

最近一個例子突顯這項先進技術的威力。攻擊者使用不完整的 QR code 發起攻擊活動，這些 QR code 被刻意截斷，底線部分缺少或模糊不清。然而，我們的引擎能夠重建這些 QR code、擷取隱藏的資訊，並在相關威脅接觸到我們的客戶之前將其攔截。這次成功證明我們的引擎有能力處理複雜的攻擊。

真實攻擊事件中的不完整 QR code 截圖



截斷的 QR code 區塊



欲了解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
欲深入了解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲深入了解賽門鐵克的端點多層次防護解決方案中「檔案檢測技術」如何保護裝置，請點擊此處。

2025/01/28

新一波Lumma惡意竊密軟體攻擊行動，使用假的圖靈(CAPTCHA)驗證機制

一個利用假的圖靈 (CAPTCHA) 驗證機制來傳送 Lumma 惡意竊密軟體的攻擊行動已被回報。這個攻擊行動鎖定的對象來自世界各地 (阿根廷、哥倫比亞、美國、菲律賓等) 和各行各業 (例如：金融機構、醫療保健、行銷和電信組織)。初始攻擊鏈始於受害者瀏覽一個已遭入侵的網站，該網站會將受害者導向一個假的圖靈 (CAPTCHA) 驗證頁面，並附上說明。網站訪客會被引導複製／貼上指令到 Windows 執行的命令提示中，接著會從遠端伺服器下載並執行 HTA 檔案。一旦 HTA 檔案執行，就會啟動 PowerShell 指令來執行其他指令碼，進而解碼並載入 Lumma 惡意竊密軟體的有效酬載。此惡意軟體是一種強大的工具，具有先進的迴避技術和資料竊取機制。

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.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。

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：

- Downloader
- Infostealer.Limitail
- Scr.Malcode!gdn32
- 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.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。

2025/01/27

《俠盜獵車手6》被拿來當釣餌：惡意軟體偽裝成封測版

熱門遊戲的炒作往往成為網路犯罪的溫床，《俠盜獵車手 6 》也不例外。Rockstar Games 的經典開放世界動作冒險系列中備受期待的下一部作品。該遊戲於 2023 年 12 月正式宣佈，將於 2025 年底推出 PlayStation 和 Xbox 版本。

2025 年 1 月，一名攻擊者在 GitHub 上建立一個儲存庫，並宣稱透過一個名為 Grand-Theft-Auto-VI-Early-Alpha-main.zip 的壓縮檔就能提早嘗鮮新的遊戲。然而，這些內容並不是封測版，而是設定好的惡意軟體。

維基百科知識：《俠盜獵車手 VI》（英語：Grand Theft Auto VI) 是由 Rockstar Games 發行的開放世界動作冒險遊戲，是繼《俠盜獵車手 V》後睽違十二年的系列正作，也是《俠盜獵車手》系列第八部主要遊戲作品。遊戲將於 2025 年秋季登陸 PlayStation 5 及 Xbox Series X／S 平台。

壓縮檔內含一個檔名為 GTAVIAlphaInstallerV1.3.exe 的可執行檔，以及一個包含欺騙性安裝指示的讀我檔案 (reademe)。讀我檔案引誘受害者：

- 下載安裝程式
- 確認已安裝 DirectX 12
- 停用他們的防毒軟體 (聲稱防毒軟體會對該遊戲產生誤報)

這種社交工程的設計目的是繞過安全防禦，讓使用者在不知情的情況下安裝 Blank Grabber(一種竊取憑證的惡意軟體)。此惡意軟體會擷取敏感資料，例如：瀏覽器儲存的密碼、cookie 和 session tokens。按照讀我檔案中指示停用防毒軟體，是確保惡意軟體執行不被發現的關鍵步驟。

透過在 GitHub 上託管惡意套件庫，攻擊者利用平台的信譽使詐騙看似合法。

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.Untrst-RunSys!g1
- ACM.Ps-Mshta!g1
- ACM.Mshta-Http!g1
- ACM.Ps-Reg!g1
- ACM.Ps-Enc!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.SuspBeh!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：

- Scr.Malcode!gen129

2025/01/27

職場焦慮助長網路釣魚：電子郵件憑證如臨大敵

最近有起網路釣魚行動利用職場上的恐懼和急迫感，試圖竊取電子郵件憑證。初始攻擊起於一封標題為「Employment Termination lists and new admin position 2025」(*解雇名單及新管理職位) 的電子郵件，以及偽裝成重要工作文件的惡意 HTML 附件 (Staff Employment Termination listsPDF.html)。開啟附件後，會顯示像極了合法電子郵件登入頁面假網頁。

該頁面採用了專業的設計和簡潔的 CSS(層疊樣式表--Cascading Style Sheets，CSS 是一種標記式語言)，並加入 DocuSign 標誌和 cPanel(一種廣受認可的網站代管管理工具) 等品牌元素。這些精心設計的元素主要在提高可信度，誘騙使用者相信該頁面是真實的。登入表格會提示使用者輸入他們的電子郵件帳號和密碼，當提交時，這些憑證就會被擷取並滲出到 Telegram 的殭屍電腦。

攻擊者利用 Telegram 的 API 進行滲透，在腳本中嵌入必要的參數及數值，包括 Telegram 機器人 API 金鑰和聊天 ID。這些寫死的參數及數值可讓竊取的憑證以訊息形式傳送至攻擊者的機器人。此技術試圖避開網路監控工具，也可即時收集憑證。

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：

- Phish.ScrTgHtml!gen1

2025/01/24

CVE-2024-50603--存在雲端網路控制平臺Aviatrix Controllers的遠端程式碼執行(RCE)漏洞，已遭開採濫用

CVE-2024-50603 是存在雲端網路控制平臺 Aviatrix Controllers 的嚴重等級 (CVSS 風險評分：10.0 滿分) 的遠端程式碼執行 (RCE) 漏洞。最近有報告指出此漏洞已在真實網路情境裡遭開採濫用。此漏洞是由於對使用者所提供的輸入處理不當 (improper neutralization) 所致，如果被利用，可能會允許未經認證的遠端攻擊者執行任意程式碼。原廠已在 7.1.4191 及 7.2.4996 的修補版本中修補此漏洞。

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: Aviatrix Controller CVE-2024-50603

2024/01/24

網路釣魚即服務(PhaaS)駭客工具套件：Sneaky 2FA

被稱為 Sneaky 2FA 的網路釣魚即服務 (PhaaS) 工具套件已被觀察到以 Microsoft 365 帳戶為目標，透過傳送付款類型相關的電子郵件，引誘收件者開啟內嵌 QR code 偽造收據的 PDF，掃描後會重導向至 Sneaky 2FA 網路釣魚網頁。釣魚網站架設在遭攻擊者所操控的基礎設施上，主要是在 WordPress 網站和由攻擊者所控制的其他網域。偽造的驗證頁面會自動填入受害者的電子郵件帳號，給人一種正版官網的感覺。

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。

2025/01/24

LucKY Gh0$t勒索軟體

在威脅領域中發現一個以 LucKY Gh0$t 為名的勒索軟體駭客組織。他們所佈署的勒索軟體是源於 Chaos 的後繼新變種，會在被加密後檔案冠上 .[4個隨機字元] 的副檔名。此攻擊的媒介與手法是透過瀏覽網頁時常見的偷渡式下載，偽裝成假的 ChatGPT 桌面版本 ("ChatGPT 4.0 Full Version - Premium.zip")。

LucKY_Gh0$t 勒索 (贖金支付) 說明 (read_it.txt) 能夠讓受害者知道他們的檔案已經被加密，除非支付贖金，否則將無法存取。攻擊者聲稱他們的動機完全是為了錢，並向受害者保證付款後會提供解密工具和刪除資料，強調他們稟持盜亦有道的「信譽」值得信賴。他們指示受害者使用提供的帶有 ID 的 SESSION 與他們聯繫，並為案件指定唯一的解密 ID。該說明警告不要刪除或修改檔案，並威脅若不支付贖金就會讓受害者永無寧日，增加受害者的壓力。

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：

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.HiddenTear!g1

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**。