保安資訊--本周(台灣時間2025/05/30)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 6,900 台受保護端點上總共阻止了 5,420 萬次攻擊。這些攻擊中有 83.1% 在感染階段前就被有效阻止：**(2025/05/26)**

- 在**7萬7,800**台端點上，阻止了**2,420**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬6,500**台端點上，阻止了**620**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,600**台**Windows**伺服主機上，阻止了**610**萬次攻擊。
- 在**4萬8,600**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,300**台端點上，阻止了**86萬6,500**次嘗試掃描在**CMS**漏洞。
- 在**4萬7,500**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**7萬4,200**台端點上，阻止了**150**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**67萬9,700**次加密貨幣挖礦攻擊。
- 在**9萬6,600**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**558**台端點上，阻止了**6萬7,000**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 7,200 個受保護端點上阻止了總計 760 萬次攻擊。**(2025/05/26)**

- 使用網頁信譽情資，在 **161.3K** 個端點上阻止 **720** 萬次攻擊。
- 攔截 **17.2K** 個端點上 **251.1K** 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 **4.7K** 個端點上攔截 **132.5K** 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 **185** 個端點上攔截 **2.2K** 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。

2025/05/30

最新的PureHVNC遠端存取木馬(RAT)部署行動

據報導，真實網路情境裡出現新一波傳送 PureHVNC 遠端存取木馬 (RAT) 的網路攻擊行動。威脅者進行多階段作業，並在攻擊中使用各種元件，包括惡意 .lnk 捷徑檔、PowerShell 程式碼、JavaScript、視窗程式自動化工具：AutoIt 等。這些網路攻擊行動會假冒各種時尚品牌的工作機會或侵權主題等誘餌。已部署的 PureHVNC 有效酬載具有授予攻擊者系統存取權限的功能，也允許攻擊者上傳額外的任意元件和有效酬載到已遭入侵的端點。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen803
- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g444
- 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：

- CL.Downloader!gen111
- CL.Downloader!gen205
- CL.Suspexec!gen200
- Scr.Heuristic!gen20
- Scr.Malcode!gen
- Scr.Mallnk!gen10
- Scr.Mallnk!gen13
- Scr.xSense!gen1
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2025/05/30

Python語言撰寫的Lyrix勒索軟體

Lyrix 勒索軟體是在地下論壇新浮上檯面之 Python 語言撰寫的勒索軟體。其行為與目前大多數的勒索軟體家族類似：

- 檔案加密和資料竊取，以獲取經濟利益
- 透過識別虛擬環境的反分析功能
- 透過執行、注入或終止程序來逃避防禦措施
- 刪除磁碟區陰影複本，以防止系統還原和資料復原成功

勒索軟體的營運商會持續開發和散佈其工具的新版本和更新版本，以最大化潛在收益，而 Lyrix 也不例外。

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

2025/05/29

全新Katz惡意竊密程式以惡意軟體即服務(M.a.a.S)形式攻擊網路瀏覽器

Katz 惡意竊密程式是一款多功能的憑證竊取駭客工具，並以惡意軟體即服務 (M.a.a.S) 的營運模式提供，專為廣泛的系統偵察和資料竊取而設計。它鎖定大量的敏感資訊，包括儲存的密碼、cookie、流行網頁瀏覽器 (Chrome、Edge、Brave、Firefox) 的會話令牌、加密貨幣錢包檔案，以及透過關鍵字比對的私人密碼金鑰。該惡意竊密程式還採用螢幕擷取和剪貼簿監控等監控工具。該攻擊利用日常的線上活動，例如：釣魚電子郵件、假冒軟體下載和惡意廣告來滲入系統。感染鏈從一個包含大量混淆 JavaScript 的初始 gzip 壓縮檔案開始。這個腳本會下載經過混淆的 Base64 編碼 PowerShell 腳本，執行後會擷取一個有效酬載。此有效酬載會被解碼並在記憶體中直接執行。一旦啟動，Katz 惡意竊密程式就會與 C&C 伺服器建立永久連線，下載更多有效酬載，並將其注入瀏覽器程序。

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.Downloader!gen48
- Phish.ScptML.L
- Ransom.Zombie
- Scr.xSense!gen3
- Scr.xSense!gen11
- Trojan Horse
- Trojan.Gen.2

- Trojan.Gen.MBT
- Trojan.Whispergate
- W32.Fixflo.B!inf
- WS.Malware.1
- WS.Malware.2
- WS.Reputation.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
- 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。

2025/05/29

駭客組織：Earth Lamia，開採濫用多個SQL注入漏洞

駭客組織：Earth Lamia，利用網路應用程式的漏洞取得組織的存取權限，利用在網路應用程式上發現的各種 SQL 注入漏洞存取目標組織的 SQL 伺服器以進行資料外洩。Earth Lamia 主要針對巴西、印度和東南亞的組織，集中在金融服務、線上零售業、IT 公司、大學和各種政府單位。該駭客組織通常會修改開放原始碼的駭客工具，並將其打包成自訂載入程式，將惡意 DLL 側載到安全應用程式中，以執行 Cobalt Strike、Vshell 和 Brute Ratel 等後門程式。

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：

VMware Carbon Black 產品的防護機制：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gen1
- Backdoor.Cobalt!gm*
- Backdoor.Ratenjay
- Downloader
- Downloader.Upatre

- Hacktool
- Linux.Mirai
- Trojan Horse
- Trojan.Dropper
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Zbot
- W32.Futurax
- 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
- Heur.AdvML.D

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。

2025/05/29

假冒免費的防毒軟體下載網頁～木馬程式VenomRAT近期很活耀

最近在真實網路情境裡發現一起由木馬程式 VenomRAT 所涉入的惡意軟體攻擊行動。該惡意軟體從偽裝成免費防毒軟體下載頁面的釣魚網站散佈。所張貼的下載連結會將毫無戒心的受害者指向 Bitbucket URL，然後再重導向至 Amazon S3 bucket 上託管的惡意 .zip 檔案。除了已部署的 VenomRAT 有效酬載之外，觀察到的行動也散佈後期攻擊工具 SilentTrinity 和 StormKitty 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-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspLaunch!g221

- SONAR.SuspLaunch!g483
- SONAR.SuspPE!gen32
- SONAR.SuspStart!gen6
- SONAR.SuspStart!gen9
- 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
- Scr.Malcode!gdn14
- Scr.NSISPacker!g2
- WS.Malware.1
- WS.Malware.2
- 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
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- System Infected: Trojan.Backdoor Activity 634

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。

2025/05/29

PumaBot--有可能成為明日之星的新型殭屍網路

PumaBot 是最近在真實網路情境裡發現一款 Go 語言撰寫的全新殭屍網路。與一些較常見的殭屍網路不同，PumaBot 並非依賴掃描網際網路來尋找易受攻擊的裝置，而是透過從攻擊者 C&C 伺服器所擷取的 IP 位址清單，以非常特定的裝置為攻擊目標。殭屍網路會嘗試強制 SSH 認

證以取得存取權限。一旦進入受攻擊的裝置，惡意軟體就會建立持久性／常駐，並執行從遠端攻擊者接收到的任何任意指令。

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：

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.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。

2025/05/29

Zanubis手機／行動裝置的惡意軟體，最近很活耀

Zanubis 是一款 Android 手機／行動裝置的銀行惡意軟體，至少從 2022 年起就活躍於威脅領域。該惡意軟體已知主要針對南美洲的銀行和金融業，但隨著時間的演進也在擴大，並將盜竊虛擬卡片和加密貨幣新增到其組合中。Zanubis 通常會冒充各種合法機構進行散佈，例如：稅務機關、銀行或最近的能源公司。最新 2025 年散佈此惡意軟體的網路攻擊行動中使用更新的變種，其中包含一些程式碼修改、新的 C&C 指令以及改進的目標銀行應用程式過濾功能。

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：

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.1
- 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。

2025/05/29

惡意垃圾郵件散播行動，大肆散佈AsyncRAT惡意程式

我們最近觀察到一些惡意垃圾郵件攻擊行動利用多重下載 (從 box.com 開始) 來傳送 AsyncRAT 有效酬載。這些電子郵件的內容是一封假借建築專案潛在供應商的報價需求。電子郵件包含一個 box.com 的連結，收件者會從該連結下載一個壓縮檔。此檔案包含多個腳本，執行時會下載惡意影像檔案。該影像檔隨後負責釋放惡意 DLL。此 DLL 會完成攻擊鏈中的最終下載動作，傳送 AsyncRAT 有效酬載。

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

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-Ps!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。

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.Async!g2
- 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。

2025/05/28

Fancy Bear駭客組織開採濫用郵件系統漏洞：CVE-2024-11182，進行傳播SpyPress惡意軟體的魚叉式網路釣魚

Fancy Bear駭客組織 (又名 APT28、Sofacy、Pawn Storm、Sednit、STRONTIUM、Tsar Team 及 Threat Group-4127) 是一個俄羅斯駭客組織，利用網路郵件介面的跨網站指令碼 (XSS) 漏洞，透過魚叉式網路釣魚傳送惡意的 JavaScript 有效酬載：SpyPress，從高價值的網路郵件伺服器竊取敏感之電子郵件資料。此行動的目標是非洲、歐盟和南美洲的政府單位和國防公司。該駭客組織發送含有惡意附件或偽造網站連結的電子郵件以進行初始存取，通常會利用社交工程伎倆來欺騙受害者。MDaemon 中的零時差 XSS 漏洞 (CVE-2024-11182) 允許遠端攻擊者在受害者的 Webmail 頁面中注入惡意 JavaScript 程式碼 (已在版本 24.5.1 中修補)。

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

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

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.Malscript
- Web.Reputation.1
- Web.Reputation.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。

2025/05/28

Bofamet惡意竊密程式

Bofamet 是在真實網路情境裡新發現 Python 類型的惡意竊密程式。該惡意軟體會從遭入侵的端點收集各種資訊，包括：憑證、系統資訊、瀏覽器 cookies、Telegram 對話資料、Discord 令牌、螢幕截圖、Steam 配置文件等。收集到的資料會在 Telegram 殭屍的協助下滲出回傳給攻擊者。

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：

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
- 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：

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

2025/05/28

macOS平台出現全新AppleProcessHub惡意竊密程式

macOS 平台出現全新 AppleProcessHub 惡意竊密程式，並偽裝成系統程序。這個最近發現的惡意軟體的功能著重於資訊蒐集與外洩。遭竊取的資料包括鑰匙鏈密碼、加密貨幣錢包、SSH 資訊、GitHub 設定資料、bash 歷史等。惡意軟體由兩個獨立的元件組成--Mach-O 二進位檔和 Bash 腳本。第一個元件負責與攻擊者的 C&C 基礎架構建立連線並執行腳本，而第二個元件則具有典型的資訊竊取功能。

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
- 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。

2025/05/27

防護亮點：得力於威脅檢測平臺：STARGate提供的網頁威脅洞察力(URL Insight)，賽門鐵克解決方案能夠有效抵禦複雜攻擊鏈的威脅

專業術語解說：

STARGate(*星際之門) 是賽門鐵克安全技術與回應 (STAR：Security Technology and Response) 團隊所維運的基於機器學習、雲知識和深度內容檢查的威脅檢測平臺。其管理框架具備自動更新所有支援防護軟體的功能，無須由使用者自行更新。

在現今瞬息萬變的威脅環境中，攻擊者持續精進他們的方法，利用各種不同且通常是合法的工具，試圖規避安全措施以散佈惡意的有效酬載。這一點在我們過去幾個月來持續監測到的網路釣魚和垃圾攻擊行動上尤其明顯。

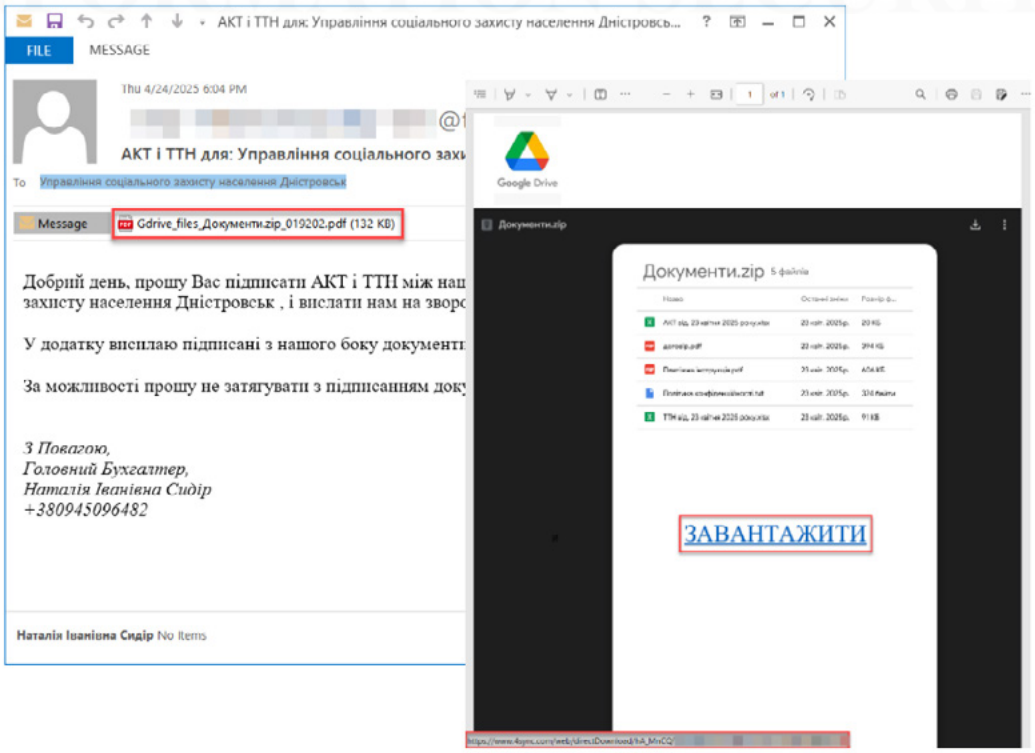
俄羅斯文的 PDF 偽造付款文件詐騙行動

自 2024 年 12 月以來，我們觀察到一波鎖定烏克蘭電子郵件地址的目標式郵件攻擊，這類攻擊使用一般的雲端儲存服務來傳送遠端存取木馬程式 (RAT)。

此類攻擊行動通常以一封包含 PDF 附件的釣魚電子郵件引爆，在某些情境中，直接在電子郵件本文中嵌入惡意網址。內嵌的惡意網址通常指向雲端硬碟平台，例如：4Sync 或 Dropbox。如果點擊這些連結，就會下載包含惡意 JavaScript 檔案的 ZIP 壓縮檔。

該 JavaScript 檔案一旦被執行，會嘗試下載和執行遠端存取工具。較早期的攻擊行動依賴 NetSupport RAT，這是一種合法的遠端管理工具，常被威脅份子濫用於隱匿存取和控制。最近的攻擊行動則轉為使用 Remote Manipulator System (RMS) Remote Utilities，顯示攻擊者的攻擊工具可能已經進化或更多樣化。

具體來說，在最新的四月攻擊中，一封附有 PDF 樣板的電子郵件會被寄出，該樣板會顯示內嵌有 4sync 網址的偽造 GDrive 內容。



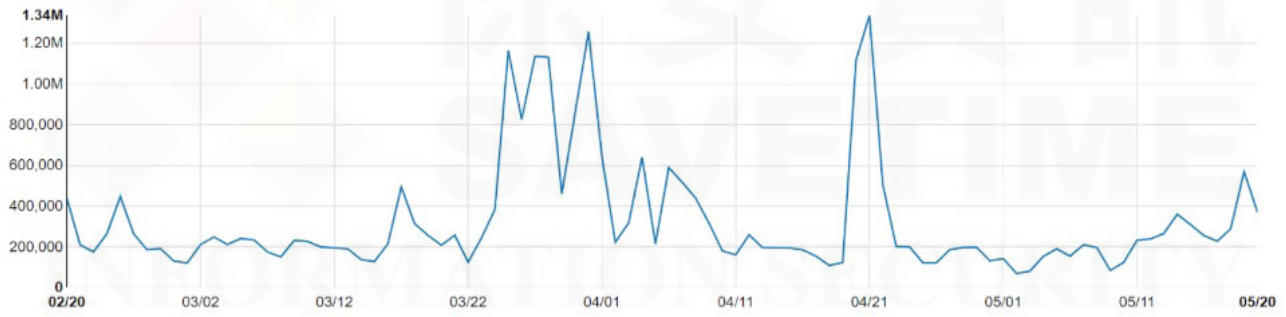
如上文所述，點選 4sync 連結會下載包含 JavaScript 檔案的 ZIP 壓縮檔。惡意 JavaScript 程式碼隨後會嘗試下載 RMS/RemoteUtilities 的 MSI 安裝程式到受害者電腦，提供遠端存取給攻擊者。

STARGate 提供的網頁威脅洞察力(URL Insight)

當 STARGate 的 URL Insight 識別出嵌入在 PDF 中的 4sync 惡意網頁，或像先前的攻擊一樣，直接嵌入在電子郵件本文中時，它會主動在攻擊鏈的初始引爆點阻止此攻擊。此攻擊會在電子郵件閘道層以 Web.Reputation.2 命名的威脅分類來封鎖，保護終端使用者不會下載攻擊者的遠端存取安裝程式。

STARGate URL Insight 負責從賽門鐵克的雲端網頁安全引擎 (WebPulse) 產出防護效益，截取具有惡意內嵌 URL 的可疑檔案或電子郵件，以及下載檔案的來源 URL。WebPulse 會對來自數千家不同企業、數百萬賽門鐵克端點防護 (Symantec Endpoint Protection) 的使用者，以及賽門鐵克電子郵件安全 (Symantec Email Security) 產品所掃描的數十億封電子郵件的 URL 進行分類與評比。這些情報是賽門鐵克豐富的威脅情報資料庫中一部分。

目前，STARGate 的 URL Insight 每日評估 Symantec Enterprise 產品中超過 30 億個網頁，且每日偵測出 20 萬個以上的**惡意內嵌網址，在攻擊行動期間 (例如：我們在 3 月和 4 月看到的攻擊行動) 更會激增超過 100 萬個**：



此外 URL Insight 可為 STARGate 其他先進技術提供更豐富寶貴的脈絡，進而實現多樣化的多層次安全方法。STARGate 的 URL Insight 價值實現也廣泛應用於賽門鐵克企業安全產品，例如：

- 賽門鐵克郵件安全雲端服務 (ESS：Email Security Service)
- 賽門鐵克地端自建郵件安全閘道 (SMG：Symantec Messaging Gateway)
- 雲端安全服務：CloudSOC
- 賽門鐵克防護引擎專為：NAS／雲端儲存
- 賽門鐵克 Sharepoint 服務防護
- 賽門鐵克雲端沙箱：Cynic

欲了解有關有效抵禦複雜攻擊鏈的威脅情資：STARGate(*星際之門) 及其支援產品的詳細資訊，請點擊此處。

欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

2025/05/27

進階持續威脅(APT)駭客集團：Swan Vector發動的攻擊行動

一個被稱為「Swan Vector」新浮上檯面的進階持續威脅 (APT) 駭客集團所發動的攻擊行動一直鎖定東亞國家，尤其是日本和台灣。此行動主要針對教育機構和機械工程產業的使用者。在魚叉式網路釣魚攻擊中，偽造履歷和財務文件作為惡意附件的誘餌。感染鏈利用 DLL 側載技術達到部署 Cobalt Strike 信標的最後階段。

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：

- Scr.Mallnk!gen*
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- 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。

2025/05/26

StarFire勒索軟體要求價值3,000美元的比特幣當為贖金

一個自稱為「StarFire」的駭客組織或個體戶最近出現在威脅環境中，以個別機器為目標散播勒索軟體。成功入侵後，Chaos 勒索軟體變種會加密檔案、冠上 .Celectial 副檔名、在多個目錄中注入勒索 (贖金支付) 通知文字檔 (StarFire-README.txt)、變更桌面桌布，並刪除磁碟區影陰複本以阻礙復原。值得注意的是，此威脅者似乎沒有進行雙重勒索--沒有資料外洩的跡象，也沒有洩露或出售竊取資訊的威脅。相反地，他們要求以 3,000 美元的比特幣當為解密贖金。

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

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/05/26

DoubleLoader惡意程式載入器

DoubleLoader 惡意程式載入器是最近在真實網路情境裡發現的全新惡意軟體家族。其主要功能與其他惡意程式載入器類似，都是從攻擊者控制的伺服器擷取惡意有效酬載，並在遭入侵的端點上執行。最近有報告指出，DoubleLoader 被部署在傳送 Rhadamanthys 惡意竊密程式等攻擊行動的初始階段。值得注意的是，DoubleLoader 使用稱為 Alcatraz 的開放原始碼混淆器來隱藏其惡意程式碼。

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：

- Downloader
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.2
- WS.Malware.1
- WS.Malware.2
- 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
- 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。

2025/05/26

另一起假冒圖靈(CAPTCHA)驗證的惡意網頁攻擊行動，傳播多種惡意竊密程式以及遠端存取木馬(RAT)

有報告指出，另一起假冒圖靈 (CAPTCHA) 驗證的惡意網頁攻擊行動，以欺騙使用者透過 Windows 執行對話框執行惡意指令。這些網頁透過釣魚電子郵件、惡意廣告或遭入侵的網站傳播，指示使用者貼上並執行啟動惡意軟體下載的指令。包括 Lumma Stealer、Rhadamanthys、AsyncRAT、Emmental 和 XWorm 在內的有效籌載會透過嵌入 MP3 等看似好的檔案之混淆腳本傳送，導致資料竊取和未經授權的遠端存取。

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

VMware Carbon Black 產品的防護機制：

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

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護 (威脅不落地)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan Horse
- Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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。

2025/05/23

Vidar和StealC惡意竊密程式，正透過社交工程伎倆大肆亂竄

趨勢科技的研究人員報告一個散佈 Vidar 和 StealC 惡意竊密程式的新一波攻擊行動。攻擊者利用 TikTok 影片的社交工程技倆，試圖引誘使用者執行任意的 PowerShell 指令。執行這些指令後，會將惡意的二進位檔傳送至受害者電腦。這兩種有效酬載都是知名的惡意竊密程式家族，用於收集和擷取使用者的各種敏感資訊。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspStart!gen6
- SONAR.SuspStart!gen9
- 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.Cobalt
- Scr.xSense!gen10
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- 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!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: Suspicious Process Accessing Lets Encrypt Certified Site
- 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。

2025/05/23

Dero惡意挖礦程式瞄準脆弱的Docker容器

據報導，有新的網路攻擊行動將 Dero 惡意挖礦程式傳送至脆弱的 Docker 容器。攻擊者在濫用無保護的 Docker API 時，會注入兩個名為「nginx」和「cloud」的惡意軟體元件。部署的 Dero 惡意挖礦程式是採用 Golang 語言撰寫，且為開源 DeroHE CLI miner 專案。被安裝在脆弱的機器上之惡意植入程式不需要與操作者的命令與控制 (C&C) 伺服器建立任何連線，因此可確保自主的傳播與操作流程。

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：

- Linux.Coinminer
- Miner.Bitcoinminer
- PUA.Gen.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。

2025/05/23

TetraLoader惡意程式載入器涉入由UAT-6382駭客組織發起的網路攻擊行動中

根據思科旗下的資安公司 Cisco Talos 最近報告指出，一起由 UAT-6382 駭客組織發起的網路攻擊行動正向受害者傳送新型的 TetraLoader 惡意程式載入器。攻擊者利用 Trimble 資產管理系統 Cityworks 存在的遠端程式碼執行 (RCE) 漏洞 (CVE-2025-0994) 進入目標環境，並執行初步偵查。一旦入侵，威脅者就會部署 AntSword 和 chinatso／Chopper 等各種 web shell，之後再用來散播後門程式。TetraLoader 是基於 Rust 的惡意軟體家族，以名為 MaLoader 的惡意軟體創作框架為基礎。一旦部署，它就可以傳送額外的任意有效酬載，例如：Cobalt Strike 或 VShell stager，這兩種有效酬載在報告的攻擊中都有被發現。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gm1
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Rustloader!gen1
- 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

網路層防護：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Audit: Bad Reputation Application Activity

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/05/22

Rhadamanthys惡意竊密程式透過網路釣魚大肆散佈

最近觀察到的網路釣魚行動中，我們看到攻擊者試圖以合法誘餌的方式傳送 Rhadamanthys 惡意竊密程式之有效酬載。在侵犯版權通知的偽裝下，攻擊者引誘受害者存取 PDF 以取得進一步詳細資訊。事實上，該 PDF 只是電子郵件中的一個連結，重導向後會嘗試下載包含 Rhadamanthys 惡意軟體的壓縮檔。此惡意軟體以 dll 的形式，透過檔案中包含的合法 PDF 檢視器應用程式進行側載。

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

自適應防護技術(包含於SESC)：

- ACM.Ps-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：

- Downloader.Trojan
- Trojan.Gen.MBT
- Trojan.Gen.2
- 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。

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**。