保安資訊--本周(台灣時間2025/06/27)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 7,100 台受保護端點上總共阻止了 5,220 萬次攻擊。這些攻擊中有 83.7% 在感染階段前就被有效阻止：**(2025/06/23)**

- 在**7萬9,400**台端點上，阻止了**2,440**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬6,100**台端點上，阻止了**590**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,500**台**Windows**伺服主機上，阻止了**580**萬次攻擊。
- 在**4萬6,500**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬300**台端點上，阻止了**73萬8,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬900**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**6萬4,800**台端點上，阻止了**130**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,400**台端點上，阻止了**68萬6,700**次加密貨幣挖礦攻擊。
- 在**10萬9,400**台端點上，阻止了**790**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**464**台端點上，阻止了**7萬5,100**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 23 萬 3,500 個受保護端點上阻止了總計 100 萬次攻擊。**(2025/06/23)**

- 使用網頁信譽情資，在 **224.2K** 個端點上阻止 **950** 萬次攻擊。
- 攔截 **24.3K** 個端點上 **353.4K** 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 **6.7K** 個端點上攔截 **180.4K** 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 **372** 個端點上攔截 **4.8K** 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。

2025/06/26

勒索軟體生態圈出現新秀：Dire Wolf駭客組織

在真實網路情境裡發現勒索軟體駭客組織：Dire Wolf。該駭客組織攻擊的目標主要集中在製造業和科技產業。已部署的勒索軟體是以 Golang 程式語言編寫，並使用 UPX 打包。該惡意軟體會加密使用者資料，並冠上 .direwolf 副檔名。Dire Wolf 勒索軟體還能夠停用各種系統服務和程序，以及刪除受感染端點上的備份和卷影副本。該威脅組織還採用雙重勒索策略，不僅會加密檔案，還會威脅受害者，如果不乖乖配合支付贖金，就會公開已遭竊的資料。

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-Sc!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Cryptlocker!g38
- SONAR.Cryptlocker!g42
- SONAR.RansomPlay!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250

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.DireWolf
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.9
- WS.Malware.2

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

2025/06/26

假免費工具之名，初始存取掮客(IAB)正在運用開放原始碼工具發動針對非洲金融業的目標式攻擊

Palo Alto 的研究人員最近公布一場針對非洲各地金融機構仍在持續進行中的攻擊行動。攻擊者散佈各種開放原始碼工具，通常宣傳為滲透測試或遠端管理工具，包括 PoshC2、Chisel 或 Classroom Spy。該威脅者先前的攻擊也顯示使用 MeshAgent，這是另一種遠端管理軟體。部署的工具通常會偽裝成合法的系統程序或第三方應用程式。攻擊者試圖使用擬部署之安裝檔的慣用圖示和名稱來偽裝它們。據信，此攻擊活動是由初始存取掮客 (Initial Access Broker-IAB) 所為，他們試圖取得易受攻擊網路的存取權限。

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：

- Hacktool.Chisel
- Infostealer

- PoshC2
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- 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。

2025/06/25

Prometei殭屍網路不斷演變，並推出可自我更新的Linux變種

根據 Palo Alto Networks Unit 42 最新報告指出，Prometei 殭屍網路已重出江湖並且功能更強化，尤其是其 Linux 的版本 (v3 和 v4)。Prometei 以挖掘 Monero 幣和竊取憑證而聞名，它採用自我更新機制和網域生成演算法 (DGA) 來增強其彈性並保持持續的 C&C 連線，即使現有的網域被關閉也是如此。此多重模組化惡意軟體使用 UPX 包裝進行混淆，可執行暴力攻擊、開採濫用已知漏洞、進行橫向移動並最終完成資料外洩。儘管這種惡意軟體擁有先進的技術，但其攻擊行動仍以財務為動機，並未歸咎於國家級的駭客。

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.Mirai
- Trojan.Gen.2
- 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。

2025/06/25

NightSpire勒索軟體

2025 年 3 月至 6 月期間，NightSpire 勒索軟體駭客集團宣稱對 33 個國家 64 個機構發動攻擊，受害者遍布全球。

美國是受影響最嚴重的國家，其次是土耳其、香港、日本、台灣、墨西哥、西班牙和埃及等地的攻擊活動，這些地區都有多位受害者。這些受害者的組織類型和規模各不相同，從小型區域性公司到與政府有關的機構，不一而足。

目標產業涵蓋公共和私人領域，包括：

- 醫療保健（醫院和醫療機構）
- 教育與政府 (學區、教育部門和市政網站）
- 金融與諮詢（投資公司、會計機構、小額信貸公司）
- 工業和製造業（包括鋼鐵、紡織、電子和專用設備）
- 酒店和旅遊業（酒店和旅遊相關業務）
- IT 服務和技術（中小企業、代管、軟體開發商和諮詢）
- 物流與運輸（港口營運商與物流公司）

NightSpire 展現出一系列與現代勒索軟體操作一致的技術。它透過命令列介面 (T1059) 執行，並依賴 DLL 側載 (T1574.002) 和進程注入 (T1055) 來實現持久性和權限提升。

為了規避偵測，該惡意軟體採用多種混淆方法，包括 AES、RC4 和 XOR 加密 (T1027)，以及軟體加殼 (T1027.002) 和偽裝成合法檔案 (T1036)。此外，它還會在執行時解碼其有效酬載 (T1140)。

它使用標準網路協定 (T1071) 進行通信，執行 DNS 查詢 (T1095)。其主要影響是資料加密 (T1486)，並將帶有「.nspire」副檔名檔案和勒索信「_nightspire_readme.txt」注入到各個目錄中。

該通知簡短而直接，告知受害者他們的敏感資料已被竊取並加密。通知要求受害者在三天內付款，並警告說，如果不遵守，將導致資料外洩事件被公告周知，被盜資料將被洩露。

洋蔥加密網址：

- nspireyzmvapgiwgtuoznlafqvlyz7ey6himtgn5bdvdcowfyto3yryd[.]onion
- a2lyiiaq4n74tlgz4fk3ft4akolapfrzk772dk24iq32cznjsmzpanqd[.]onion
- nspirebcv4sy3yydtaercuut34hwc4fsxqqv4b4ye4xmo6qp3vxhulqd[.]onion
- nspiremkiq44zcxjbgvab4mdedyh2pzj5kzbmvftcugq3mczx3dqogid[.]onion

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：

- Ransom.NightSpire

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2025/06/25

婚禮邀請詐騙在印度安卓行動裝置上部署SpyMax遠端存取木馬(RAT)

一項名為「Wedding Invitation* 婚禮邀請」的安卓行動裝置網路釣魚行動被發現針對印度各地的行動用戶，透過 WhatsApp 和 Telegram 傳送帶有間諜軟體 .APK 的 APP 獨立安裝檔。根據 K7 Computing 的報告，這些惡意 APP 偽裝成數位婚禮邀請函，誘騙用戶安裝被加料的惡意 .APK的 APP 獨立安裝檔。安裝後，該 APP 會秘密部署 SpyMax RAT 或類似的間諜軟體，這些惡意軟體能夠隱藏其圖示，在啟動時自動執行並收集簡訊、聯絡人、通話記錄、按鍵和一次性密碼 (OTP) 等敏感資料。被盜資料會透過 Telegram 機器人或命令與控制伺服器洩漏給攻擊者。

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：

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

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。

2025/06/24

防護亮點：假冒收費道路與州政府的簡訊釣魚行動

簡訊釣魚已成為網路罪犯針對個人一種日益普遍的方法。其中一個演進趨勢是在這些簡訊釣魚行動使用與運輸相關的主題。這些主題包括收費道路系統和政府機構，例如汽車管理局 (DMV)。本則防護亮點將討論這些簡訊釣魚行動、它們如何運作，以及賽門鐵克如何防禦以交通為主題的簡訊釣魚。

假冒收費道路和運輸系統的網路釣魚行動

假冒收費道路的網路釣魚行動，讓詐騙分子發送看似來自收費道路當局或政府機構 (例如：美國各州 DMV 或交通部 (DOT)) 的簡訊通知。這些簡訊聲稱收件人尚有未支付的通行費或未付的交通罰單，並威脅如果未付罰款，就會被加重罰款和暫時吊銷駕照。並提供「支付」罰款的網址連結。

這些網路釣魚行動是如何運作的？

許多不同的收費道路和州政府運輸部門在這些網路釣魚行動中被冒用。舉例如下：

- 收費道路
  - e-zpass.com-refundio.xyzE-ZPass（美國境內 20 個州收費機構的統一系統）
  - 407etr.com-wyei.vip407 ETR（加拿大安大略省）
  - bayareafastrak.org-etcnp.winBay Area FasTrak（北加州）
  - ezpassritba.com-nvu.win 羅德島匝道和橋樑管理局
  - ipass.com-servicesic.worldI-PASS（伊利諾伊州）
  - mypeachpass.com-ttxkj.vipPeach Pass（喬治亞州）
  - ohioturnpike.org-iggd.vip 俄亥俄州高速公路
  - sunpass.com-tollbillgav.worldSunPass (佛羅里達州)
  - thetollroads-paytollzsd.world 收費道路（南加州）
  - txtag.org-etcyq.winTxTag (德州)
- 州政府
  - mydmv.org-etcbqa.winMyDMV（許多州車管局使用的品牌）
  - dds.georgia-govke.icu 佐治亞州駕駛服務部
  - dmv.colorado.gov-nopk.icu 科羅拉多州車管所
  - ksdot.com-abvu.top 堪薩斯州運輸部
  - mass.gov-etcgn.win 馬薩諸塞州
  - michigan.gov-etcoag.vipMichigan
  - nj.mvc-govxy.icu 新澤西州汽車委員會
  - oregon.gov-ccfdrde.icuOregon
  - scdmvonline.com-tollbilltei.win 南卡羅來納州 DMV
  - transportal.wv.gov-jsbp.icu 西維吉尼亞州
  - wisconsindot.gov-etcpe.xinWisconsin DOT
  - vdot.virginia-ticketpd.xinVirginia DOT
  - utah.gov-etcpos.winUtah

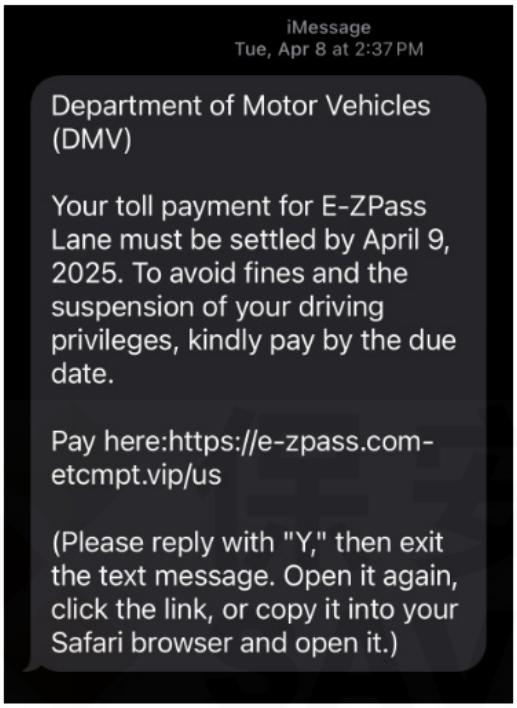
這些簡訊釣魚行動通常遵循這種模式：

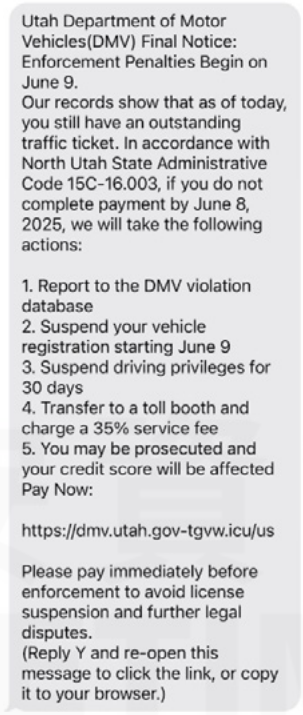
- 向目標的電話號碼傳送簡訊
- 該訊息包含一個指向偽造收費道路系統或州政府機構的類似網域的連結，該網域通常位於與收件人電話區號相對應的州內
- 收件人會被指示按照連結支付罰款，否則將面臨有風險的後果，例如：「您可能會被起訴，您的信用評分也會受到影響」和「罰款和吊扣駕照」。

- 點選該連結後會進入一個模仿官方收費道路或州政府機構網站的虛假網站。
- 虛假網站要求目標輸入個人資訊，例如：姓名、地址、電話號碼和信用卡詳細資料。
- 這些資訊隨後會被詐騙分子利用，用於身分盜竊或金融詐騙。。

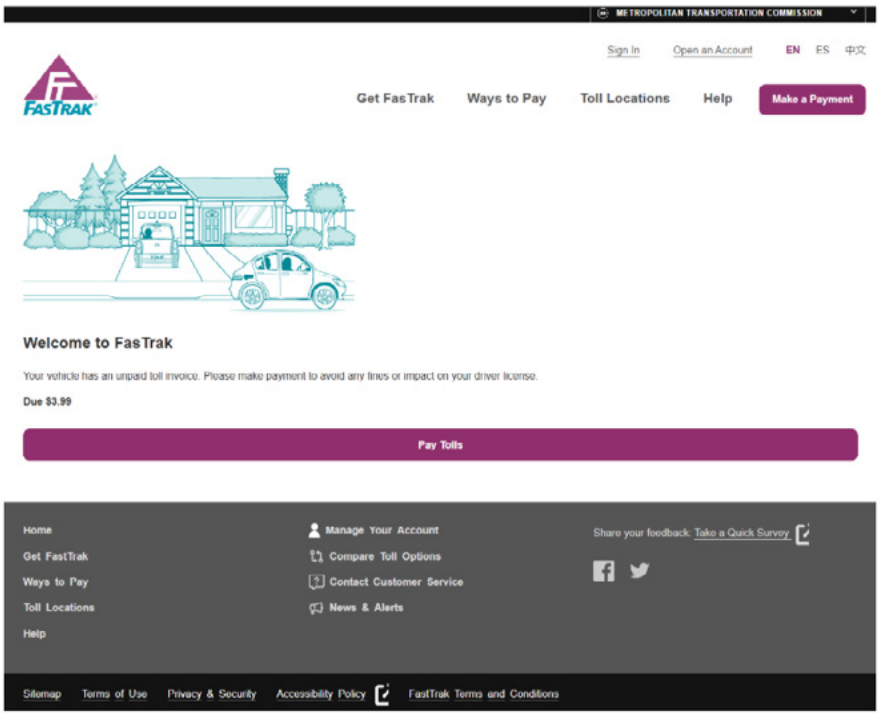
常見訊息範例

以下是一些典型的訊息：

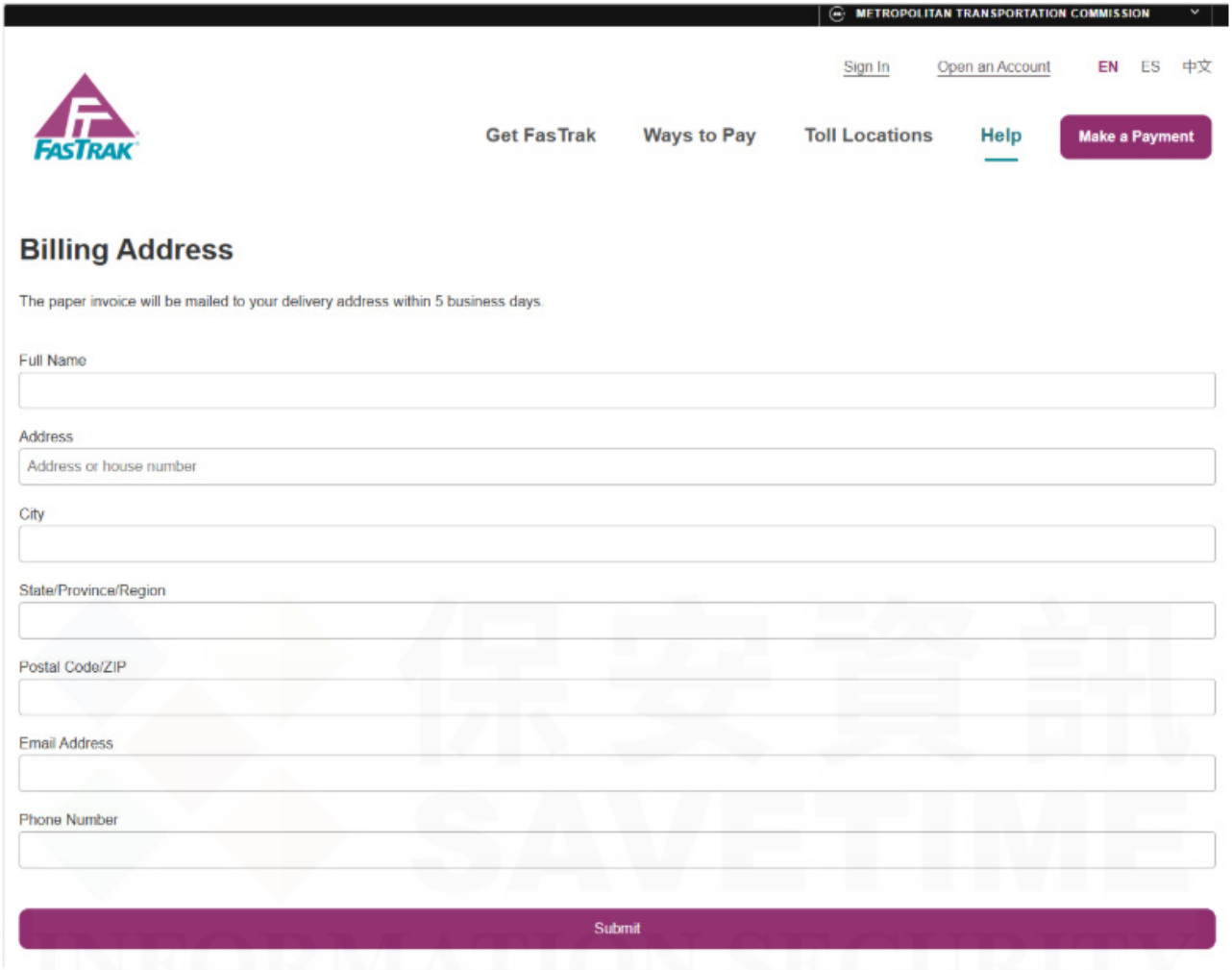




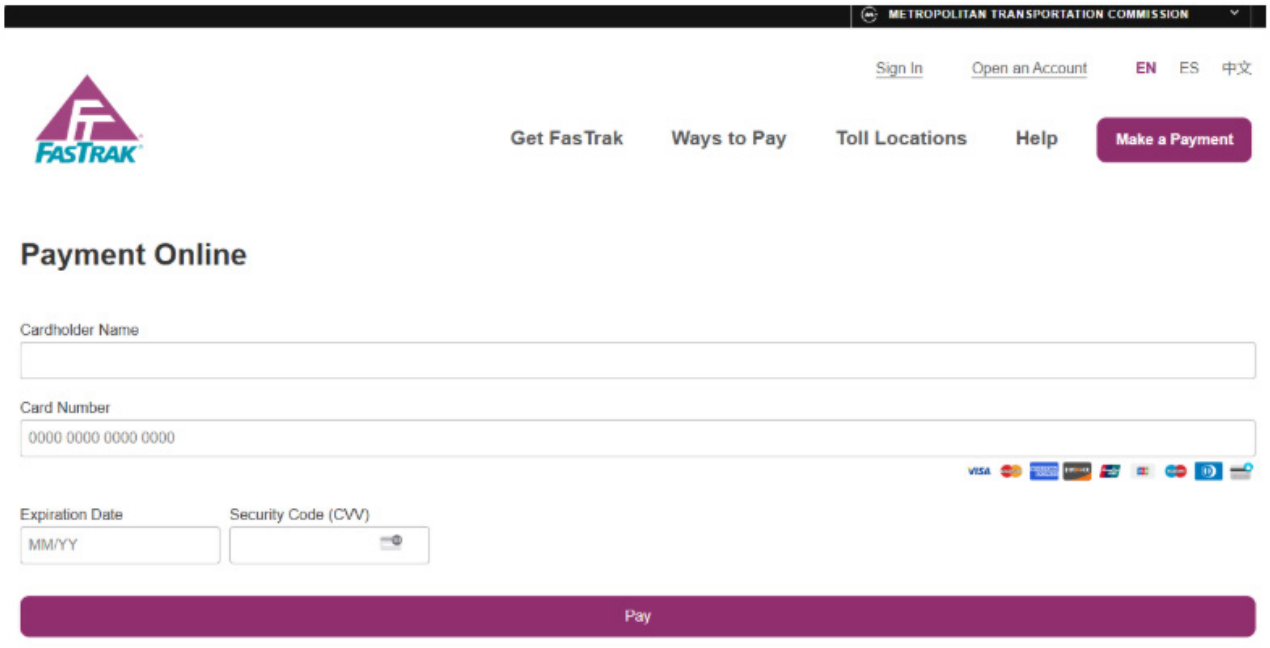
訪問這些訊息中的網站會將收件人帶入與真實網站相似的版本。例如：hxxps://bayareafastrak.org-ghec[.]vip/us/ 會引導至以下頁面：



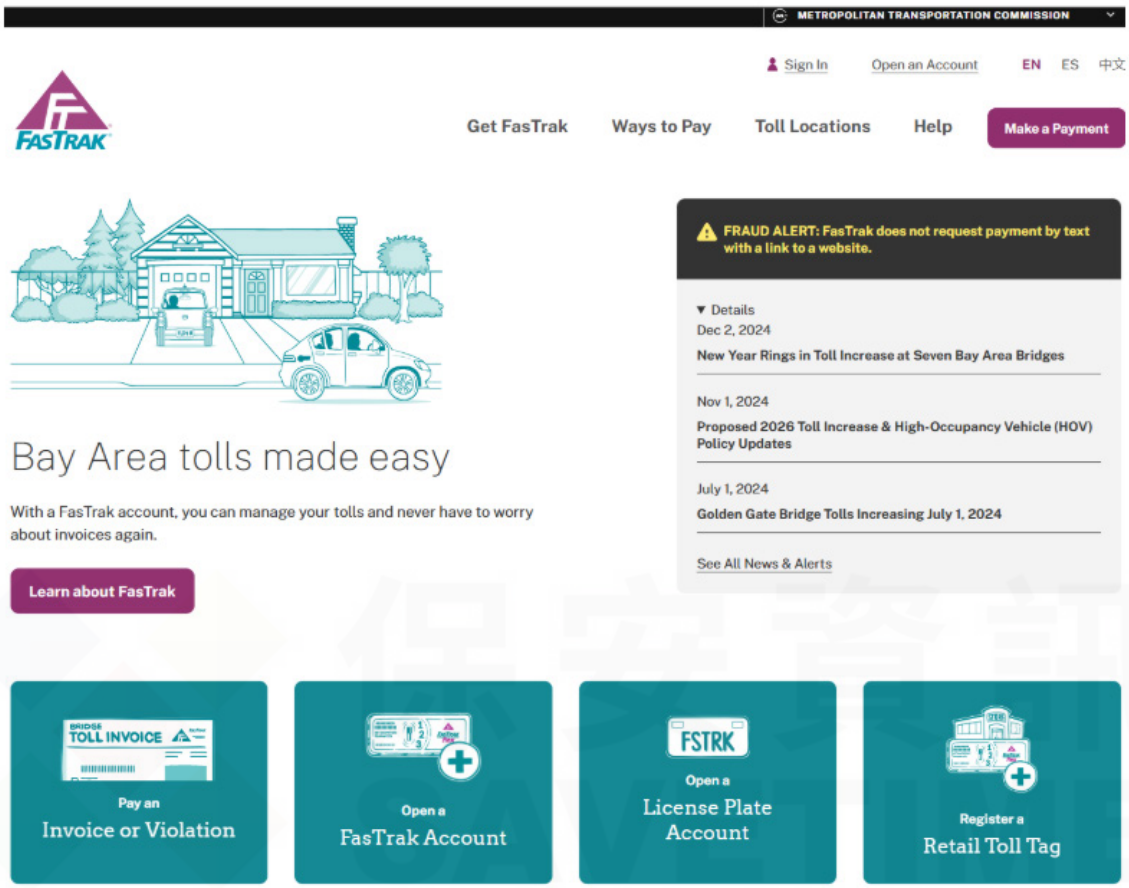
按一下「繳付通行費」連結，就會連結到這裡：



填寫表格並按一下「提交」，就會進入此頁面，要求填寫信用卡資訊：



這個偽裝的網站看起來與下圖所示的真實 FasTrak 網站極為相似。請注意，它包含一個欺詐警告，即「FasTrak 不會要求通過帶有網站鏈接的文字付款」。但偽裝的網站沒有這個警告。



以交通為主題的簡訊釣魚行動的演變

WebPulse 團隊觀察到簡訊釣魚行動的多種主題轉變。最初，註冊者使用模仿特定收費系統的網域，例如：E-ZPass。之後，他們轉移到以政府為主題的網域，與州政府機動車輛管理部 (DMV) 和交通部 (DOT) 的機構網域相關，如上文所述。

這些網域的註冊者也被觀察到獲取以包裹遞送為主題的網域，例如：

- canadapost-postescanada-help.cc(加拿大郵政)
- correoargentino.com-aris.win(阿根廷郵政)
- us-fedex.com-update.icu（聯邦快遞）
- purollator.etcbti.vip(加拿大快遞公司 Purolator)
- royalmail.com-updatecore.xin(英國皇家郵政)
- usps.paytollivub.vip(美國郵政)。

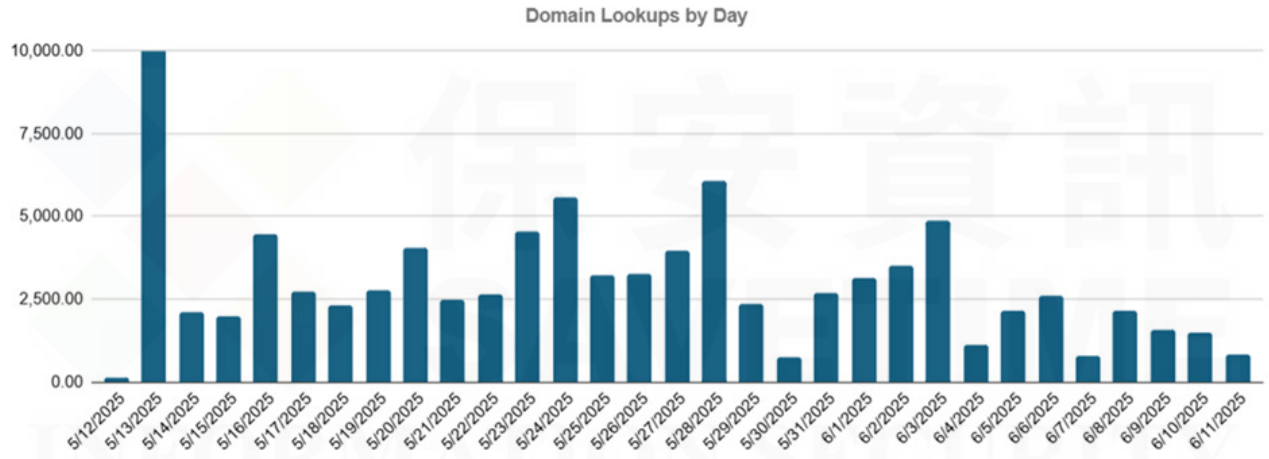
最近，WebPulse 團隊發現以金融為主題的網路釣魚網域名稱與收費道路和政府為主題的網路釣魚網域名稱之 Whois 註冊人或主機 IP 位址相同。例子如下：

- schw-ab-cc.vip
- flde-lity.com-alert.vip
- flde-lity.com-security.vip
- fide-lity-com-wa.cc

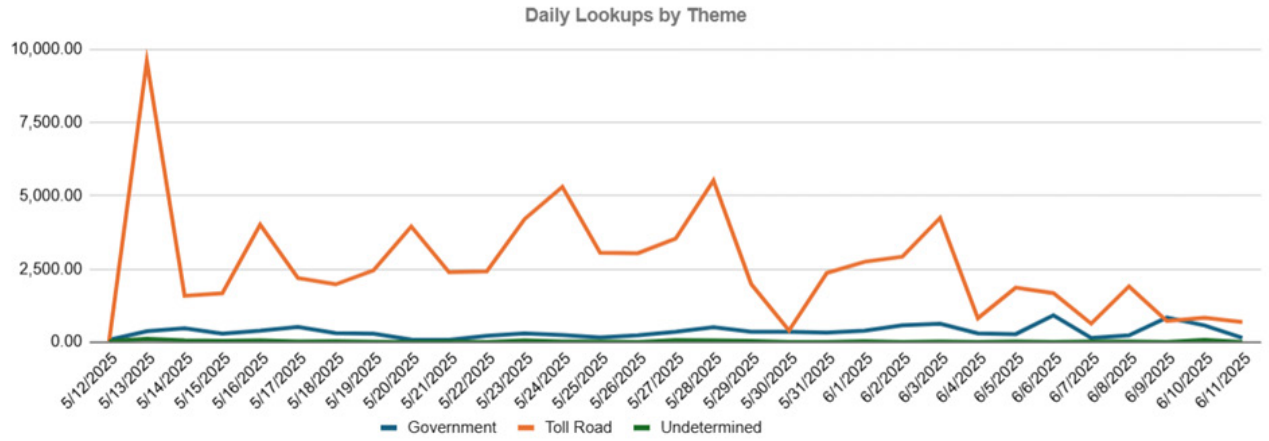
- fide-lity-com-us.top
- fide-lity-com-us.cc
- fide-lity-com-oh.cc
- fide-lity-com-nh.cc
- fide-lity-com-me.cc
- fide-lity-com-la.cc
- fide-lity-com-ky.cc
- fide-lity-com-ks.cc
- fide-lity-com-in.cc。

近期活動與趨勢

下圖顯示過去 30 天內，賽門鐵克特徵資料庫偵測到的收費道路和政府根網域的 WebPulse 每日查詢總數。



依主題、收費道路和政府 (例如：DMV、運輸部等) 來區分網域，可以發現這些趨勢。



賽門鐵克可保護您免受這些威脅的侵害，這些威脅是透過下列方式識別出來的：

- 所有啟用 WebPulse 產品的安全類別，都涵蓋觀察到的網域／IP。

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。

2025/06/23

採用Python撰寫的勒索軟體在最近行動中被大四散播

據 Tinexta 研究人員報告，在真實網路情境裡新發現一起散播 Python 類型的勒索軟體之網路攻擊行動。攻擊者利用公開存取的 GitHub 儲存庫來託管惡意 .ISO 二進位檔。散播的映像包含一個 .LNK 捷徑檔，會在受害者機器上觸發感染。勒索軟體會加密使用者資料，並灌上 .iDCVObno 副檔名。贖金備忘錄以文字檔的形式釋出，檔名為「RESTORE-MY-FILES.TXT」，建議受害者透過提供的電子郵件地址與攻擊者聯絡。該勒索軟體利用多個 VBS/BAT 腳本，以確保受感染端點的權限升級和持久性。它還具有在加密過程完成後停用卷影複本和更改桌布的功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Net!g1
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen43
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malscript
- Trojan.XSense.C
- WS.Malware.1
- WS.Malware.2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/06/23

PylangGhost--新出現Python類型的遠端存取木馬程式

PylangGhost 是 Cisco Talos 的研究人員最近發現一種新的 RAT(遠端存取木馬)。顧名思義，此惡意軟體以 Python 程式語言撰寫，與較舊的 GolangGhost RAT(遠端存取木馬) 有一些相似的程式碼和功能。該攻擊行動是由 Famous Chollima 駭客組織所為，目標是在加密貨幣和區塊鏈技術方面有經驗的個人。該駭客組織的攻擊目標鎖定在 Windows 和 macOS 兩種系統， PylangGhost 傳送至 Windows 系統，macOS 則會則感染 Golang 語言的版本。PylangGhost 具有模組化架構，攻擊者可在受感染的端點上執行各種指令、下載／上傳檔案、竊取敏感資訊等。

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

自適應防護技術(包含於SESC)：

- ACM.Ps-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：

- Backdoor.Trojan
- Infostealer
- 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。

2025/06/22

Shadow Vector：採用SVG偷渡技術的網路攻擊行動鎖定哥倫比亞用戶

根據報導，一個「Shadow Vector」網路釣魚惡意軟體散播行動偽裝成緊急法院通知的惡意 SVG 檔案攻擊哥倫比亞用戶。該行動使用 MITRE ATT&CK 已定義的 SVG 偷渡技術，即使用可縮放向量圖形嵌入或連結惡意內容。行動首先發送包含 SVG 附件的魚叉式網路釣魚電子郵件，這些附件在瀏覽器中呈現後，將受害者重導向到 Bitbucket、Dropbox 等公共平台下載有效酬載。

這些有效酬載通常是受密碼保護的壓縮檔，包含合法可執行檔和惡意 DLL。感染鏈使用 JavaScript 和 PowerShell 階段程式來啟動多階段攻擊流程，包含 DLL 側載、UAC 繞過、程序注入以及類似 Katz Loader 的惡意程式載入器。最終，該惡意軟體會遞送 AsyncRAT 和 RemcosRAT，授予攻擊者完全遠端存取權限，進而竊取憑證和鍵盤記錄，並為後續潛在的勒索軟體部署預作準備。

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.SuspDriver!g30

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.Html
- Scr.MalSvg!gen2
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Remcos
- Web.Reputation.1
- 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。

2025/06/20

Amatera惡意竊密程式

Amatera 是最近發現的惡意竊密程式，被公認為是源於舊版 ACR 惡意竊密程式的進化版。據報導，該惡意軟體透過惡意軟體即服務 (MaaS) 模式提供銷售。雖然該惡意軟體與 ACR 惡意竊密程式有程式碼重疊和相似的功能，但新導入的更新包括增強的規避和防分析機制，以及改進的竊取功能。該惡意軟體的目標是收集和滲透敏感資訊，包括：瀏覽器內儲存的資料、cookie、加密貨幣錢包、瀏覽器擴展功能、憑證、儲存在磁碟上的檔案等。惡意軟體也可能用於下載和執行任意的有效酬載或腳本。近幾個月來，Amatera惡意竊密程式大多數是透過採用 ClearFak 伎倆的行動散佈，也有使用 ClickFix 伎倆。

保安補充說明：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，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。ClearFak 攻擊手法是將惡意程式崁入網站，讓瀏覽該網站的用戶被暗中下載惡意酬載，其實屬於水坑式攻擊的一種。而會用 ClearFak 這個字眼，是崁入網站的惡意程式碼是明碼之 JavaScript。

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：

- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

- WS.SecurityRisk.3
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

2025/06/20

CVE-2025-49113--存在郵件伺服器Roundcube的後身分驗證(Post-Auth)遠端程式碼執行(RCE)漏洞

CVE-2025-4123 是近期被揭露的嚴重等級 (CVSS 風險評分：9.9) 的後身分驗證 (Post-Auth) 遠端程式碼執行 (RCE) 漏洞，會影響郵件伺服器 Roundcube，這是一個免費的開放原始碼 webmail 應用程式。成功開採濫用此漏洞能讓經認證後的使用者透過 PHP 物件反序列化漏洞執行遠端執行程式碼。原廠已在 1.6.11 版本修補此漏洞。CVE-2025-4123 也被回報已在在真實網路情境裡被大肆開採濫用。

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: Roundcube Webmail CVE-2025-49113

2025/06/20

Discord提供的自訂邀請機制遭濫用於惡意軟體攻擊行動，注入AsyncRAT遠端存取木馬和Skuld惡意竊密程式

一個鎖定加密貨幣使用者以獲取經濟利益的新型複雜惡意軟體攻擊行動，正濫用 Discord 邀請系統中一個細微的弱點，散佈一個稱為 Skuld 和 AsyncRAT 的惡意竊密程式。目標受害者主要集中在奧地利、法國、德國、斯洛伐克、越南、荷蘭、美國和英國。此攻擊行動濫用 Discord 的機制，讓攻擊者能重用失效或被刪除的邀請碼來建立自訂網址，藉此將原本可信任的來源重新導向至惡意伺服器。

底層的漏洞源於於 Discord 的自訂邀請連結機制。雖然該平台不允許原本伺服器重新使用過期或刪除的邀請碼，但卻可以用自訂網址重新利用那些已經失效的代碼。此漏洞能讓威脅份子

「劫持」曾受信任的邀請連結 (例如：從舊的論壇文章或部落格)，並暗中將使用者重導向至他們自己的惡意 Discord 伺服器。使用者在不知情的情況下透過被劫持的連結加入惡意 Discord 伺服器時，會被提示完成「驗證」步驟。這包括與機器人互動，機器人會將用戶引導至一個假冒網站，該網站有一個顯眼的「驗證」按鈕。按一下此按鈕就會觸發惡名昭章的 ClickFix 社交工程策略，將 PowerShell 指令複製到使用者的剪貼簿。然後會指示使用者將此「驗證字串」貼入 Windows 執行對話方塊，並按 Enter。執行此指令會啟動感染下一階段，最終注入兩個主要有效酬載--AsyncRAT 和客製化 Skuld 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-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- 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.ASync!g2
- Trojan Horse
- Trojan.Gen.MBT
- Scr.Malcode!gdn14
- Scr.xSense!gen3
- 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。

2025/06/20

Minecraft遊戲玩家遭到鎖定，駭客假借提供修改工具發動竊取帳密資料攻擊

根據 Checkpoint 最近一份報告指出，由 Stargazers Ghost Network 所發動的大規模惡意軟體行動正大肆鎖定 Minecraft 玩家。這些惡意修改工具 (mod) 偽裝成各種作弊與自動化工具，並透過 GitHub 儲存庫散佈。攻擊鏈首先是以 Java 類型的下載程式，偽裝成熱門的 Minecraft 作弊程式，接著是以 Java 和 .NET 為基礎的惡意竊密軟體，從受感染的 Windows 裝置擷取憑證、驗證代碼和加密貨幣錢包。我們強烈建議玩家從未經驗證的來源下載修改工具 (mod)時 務必謹慎，並持續注意所涉及的重大網路安全風險。

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.Dropper
- SONAR.Stealer!gen1
- 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：

- Backdoor.Bifrose
- Downloader
- Trojan Horse
- 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!100

- Heur.AdvML.B!200
- Heur.AdvML.B

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。

2025/06/20

下載應用程式安裝檔務必從原廠網站～被植入惡意程式的MSI安裝檔正在散播XWorm RAT特洛伊木馬

據報導，與中國有關聯的威脅份子散佈偽裝成 WhatsApp 安裝檔的特洛伊木馬的 MSI 安裝程式，以散布經客製化的 XWorm 遠端存取特洛伊木馬程式 (RAT)，目標是東亞和東南亞的使用者。攻擊鏈包括嵌入在影像檔中的加密 shellcode、透過工作排程執行 PowerShell 腳本以及 shellcode 惡意程式載入器。最後有效酬載是經修改後的 XWorm RAT，其增強偵測 Telegram 安裝的功能，並透過 Telegram 機制回報受感染的系統。

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：

- Scr.Malcode!gdn14
- Scr.Malcode!gdn20
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.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

- Heur.AdvML.B
- 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
- 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。

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**。