保安資訊--本周(台灣時間2025/02/21)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 38 萬 5,600 台受保護端點上總共阻止了 4,430 萬次攻擊。這些攻擊中有 82% 在感染階段前就被有效阻止：**(2025/02/17)**

- 在**7萬9,200**台端點上，阻止了**1,470萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬5,500**台端點上，阻止了**640萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬6,300**台**Windows**伺服主機上，阻止了**640萬**次攻擊。
- 在**4萬9,800**台端點上，阻止了**180萬**次嘗試掃描伺服器漏洞。
- 在**9萬4,000**台端點上，阻止了**71萬7,000**次嘗試掃描在**CMS**漏洞。
- 在**4萬8,700**台端點上，阻止了**250萬**次嘗試利用的應用程式漏洞。
- 在**11萬700**台端點上，阻止了**240萬**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**91萬2,400**次加密貨幣挖礦攻擊。
- 在**10萬4,900**台端點上，阻止了**8萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**472**台端點上，阻止了**8萬1,700**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 15 萬 6,200 個受保護端點上阻止了總計 740 萬次攻擊。**(2025/02/17)**

- 使用網頁信譽情資，在 **149.4K** 個端點上阻止 **690** 萬次攻擊。
- 攔截 **18.9K** 個端點上 **322.8K** 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 **5.8K** 個端點上攔截 **103.4K** 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 **190** 個端點上攔截 **3.8K** 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。

2025/02/20

Bookworm惡意軟體涉入駭客組織Fireant(又名 Stately Tarurus)針對東南亞國家的攻擊活動

在 Palo Alto Networks 最近發表一份報告中，根據駭客組織 Fireant(又名 Stately Tarurus) 影響東南亞國家的網路攻擊活動，發現 Bookworm 惡意軟體涉入其中。根據報告，Bookworm 是 2015 年首次問世的模組化特洛伊木馬，之前並沒有隸屬於任何組織。最初的 Bookworm 惡意軟體利用 DLL 測載來解密和啟動攻擊者 shellcode。在最近後繼版本中，shellcode 的格式變更為 UUID 字串，然後被解碼為二進位資料，並透過合法的 API 函式啟動，完全捨棄使用側載。

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。

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.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

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。

2025/02/20

ACR Stealer惡意竊密軟體利用固定情報解析器(Dead Drop Resolver-DDR)技術

ACR Stealer 惡意竊密軟體是採用 C++ 撰寫，最初發現於 2024 年初。該惡意軟體以惡意軟體即服務 (MaaS) 的形式進行銷售。ACR Stealer 被認為是源於較舊版本 GrMsk Stealer 的最新後繼版本。從功能上看，該惡意軟體的目標是收集和滲出各種敏感資料，包括系統資訊、憑證、瀏覽器 cookies、第三方應用程式的配置檔案、加密貨幣錢包等。ACR Stealer 利用稱為固定情報解析器 (Dead Drop Resolver-DDR) 的網頁服務技術，將合法網站做為 C&C 的媒介，從中擷取實際惡意 C&C 伺服器的解析位址。最近例子像是一些合法網站被當作 C&C 媒介，包括 Steam 遊戲入口網站、Google Docs 和 Telegra.ph 部落格平台。

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
- 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：

- Trojan.Gen.MBT
- Trojan Horse
- 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
- 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：

- 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。

2025/02/20

駭客組織RedCurl(也稱為EarthKapre)近期發動的APT網路攻擊活動

駭客組織 RedCurl(也稱為 EarthKapre) 向來以發動間諜及資料滲透活動而聞名。最近觀察到的威脅活動屬於此威脅份子利用合法 Adobe 可執行檔 (ADNotificationManager.exe) 來側載惡意二進位檔案。感染鏈是透過精心製作的 PDF 惡意垃圾郵件，引誘啟動 ZIP 壓縮檔內的 .img 二進位檔案而啟動。在執行／掛載 .img 檔案時，惡意 .dll 二進位檔會被側載到已遭入侵的端點。成功感染後，據觀察，威脅者會執行 SysInternals Active Directory Explorer (AD Explorer) 工具進行資料收集，之後再利用 Cloudflare Workers 基礎架構進行 C&C 目的。

網路上知識：Active Directory Explorer (AD Explorer) 是進階 Active Directory (AD) 檢視器和編輯器。您可以使用 AD Explorer 輕鬆地巡覽 AD 資料庫、定義我的最愛位置、檢視物件內容和屬性，而不需要開啟對話方塊、編輯權限、檢視物件的架構，以及執行您可以儲存和重新執行的複雜搜尋。Sysinternals 是 Windows 平臺上相當實用的工具集，能提供豐富詳實的資訊，協助系統管理員更有效率處理各種問題。AD Explorer 是 Sysinternals 內含的工具軟體。

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.Malimg

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。

2025/02/20

CipherLocker勒索軟體

CipherLocker 是在真實網路情境上發現的全新勒索軟體。該惡意軟體會加密使用者資料，並在被加密檔案冠上 .clocker 副檔名。勒索 (贖金支付) 通知會以「README.txt」文字檔的形式存在，並包含對受害者的指示，包括攻擊者的電子郵件聯絡方式。CipherLocker 能夠刪除受感染端點上的陰影副本和備份檔案。

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.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!200
- Heur.AdvML.C

2025/02/19

客服人員有很高的機率成為資安破口：Zhong Stealer惡意竊密程式，透過社交工程伎倆傳播

Zhong Stealer 惡意竊密程式，最近涉入針對金融科技和加密貨幣領域的散佈行動。攻擊者利用線上聊天平台向各種支援團隊建立服務案號，並向毫無戒心的支援人員提供包含惡意二進位檔案的 .zip 壓縮檔案。以這種方式散佈其中一個有效酬載是 Zhong Stealer 惡意竊密程式，威脅者利用它從受感染的端點收集並外流機密資料，例如：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：

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!gdn32
- 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!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)：

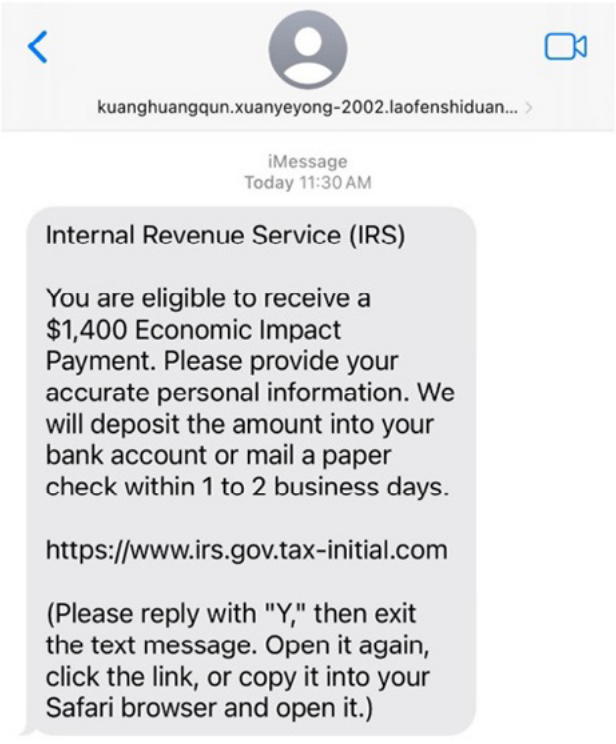
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/02/18

防護亮點：賽門鐵克的網頁生態即時情資系統--WebPulse，監控可疑美國國稅局(IRS)與稅務相關的網路活動

在美國，1 月到 4 月被視為報稅季，隨著報稅季來臨，我們看到與美國國稅局 (IRS) 及稅務相關的網路活動惡意網路活動以及新網域名稱註冊增多了。

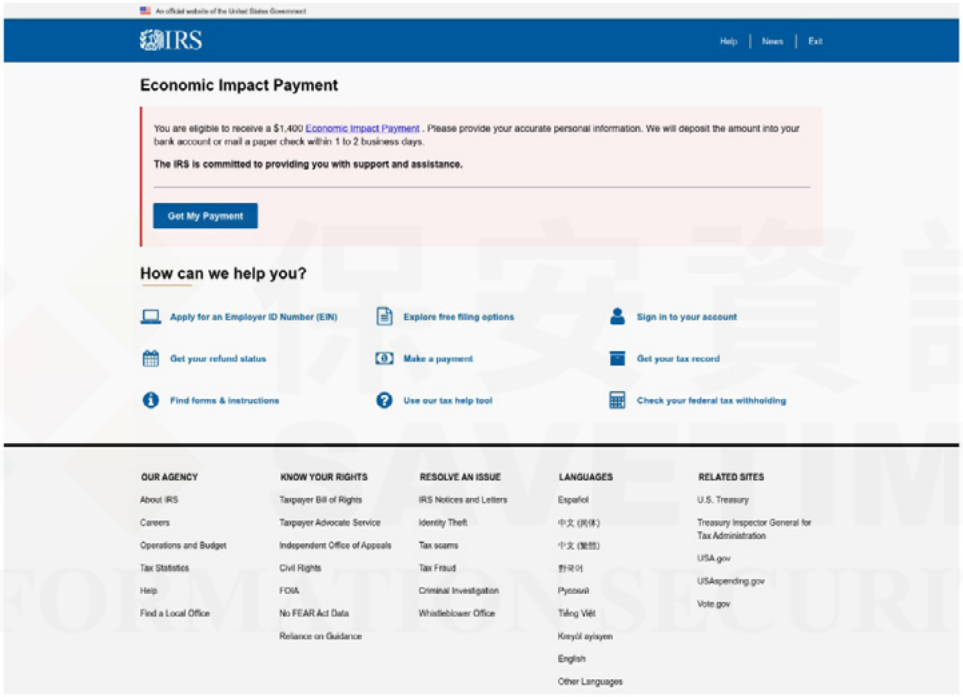
例如：這個 hxxps://www.irs.gov.tax-initial[.]com 的網址鏈結是在 1 月 27 日傳送：



在賽門鐵克的網頁生態即時情資系統--WebPulse 的遙測大數據中尋找該網域模式，發現許多類似的網域。例如：

- irs.gov.reporting-tax[.]com
- irs.gov.responsibilities-tax[.]com
- irs.gov.tax-initial[.]com
- irs.gov.tax-winnings[.]com
- irs.gov.tax-ownership[.]com
- irs.gov.ownership-tax[.]com。

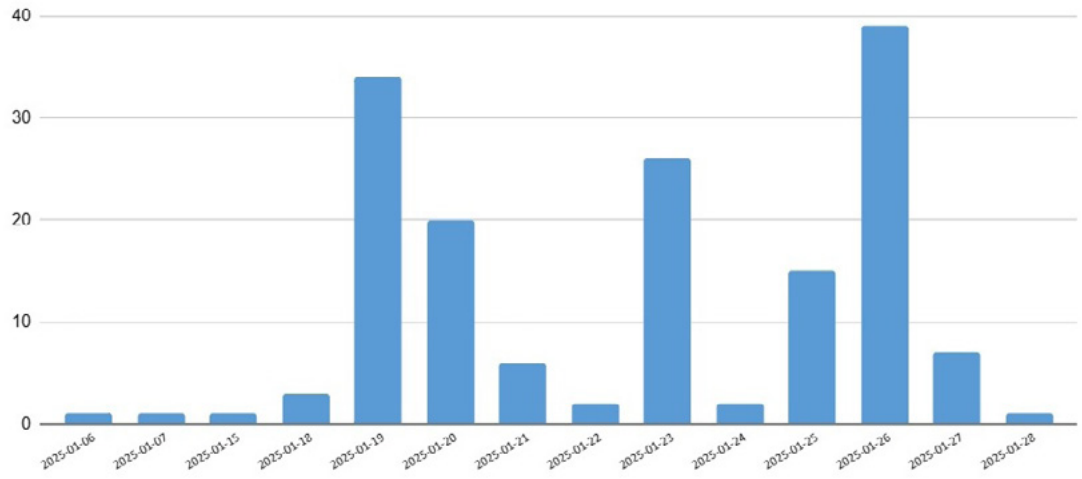
WebPulse 的遙測大數據顯示，這些網域名稱在釣魚訊息和社交媒體上都曾出現。點擊這些連結，會連結到偽造成 IRS 內容的網站，例如：在 irs.gov.tax-private[.]com 所發現如下這個頁面：



檢視 2025 年 1 月「irs.gov.*」子網域的 pDNS 資料，發現有 158 個特定網域。下圖顯示一月份每天初次出現此樣式的特定網域數量。

*開發保護性網域名稱服務 (Protective Domain Name System，PDNS)

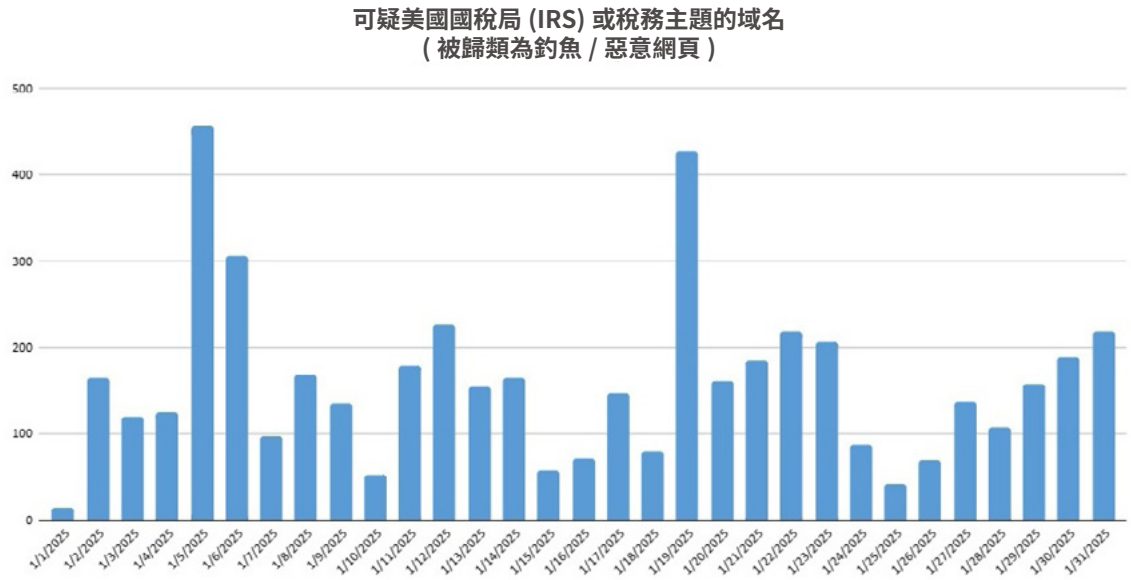
每天初次出現「irs.gov.*」子網域樣式的特定可疑網域數量



在 2025 年 1 月，我們在 Webpulse 遙測大數據中擴大搜尋其他可疑美國國稅局 (IRS) 或稅務主題的活動，發現將近3500個特定可疑美國國稅局(IRS)或稅務主題的域名被歸類為釣魚／惡意網頁，例如：

- 2024-tax-refund[.]info
- claim[.]tax[.]refund[.]drtf5pe[.]us
- claim[.]tax[.]refund[.]eljungle[.]me
- claim[.]tax[.]refund[.]ema0jrm[.]us
- claim[.]tax[.]refund[.]encengojos[.]live
- form[.]e-refund[.]irs[.]gov[.]matheusmartins[.]website
- irs-claim-covid[.]com
- irs-claim-federal[.]com
- irs-claim-financial-profile[.]com
- irs-claim-government[.]com
- irs-claim-grant[.]com
- irs-claim-grants-governemnt-us[.]com
- irsclaim-kecv[.]mtzyxx[.]mobi
- payment[.]claim-irs-us[.]com
- payment[.]irs[.]benefit[.]marypoesia[.]com
- payment[.]irswebsecure[.]com
- paymentax[.]top
- payment-form-irs[.]com
- your[.]irs[.]gov-addpayment[.]info
- your[.]irs[.]gov-confirmaccess[.]info
- your-gov-tax[.]completissuc[.]club

下圖顯示每天賽門鐵克的網頁生態即時情資系統--WebPulse 有 3,500 個網域的查詢總次數：

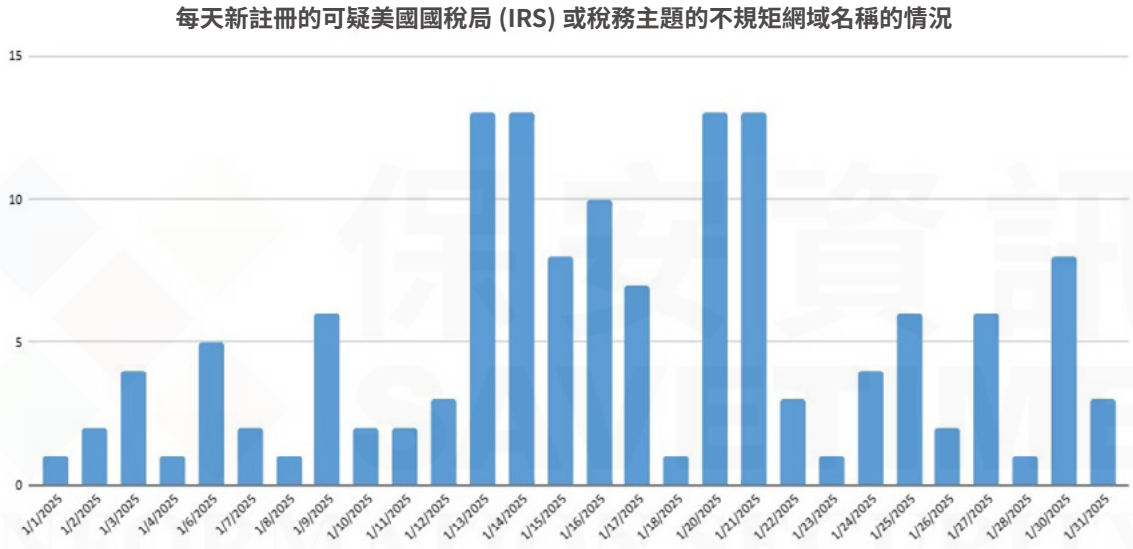


檢視 2025 年 1 月以美國國稅局 (IRS) 和美國聯邦稅務為主題的新網域名稱註冊，發現有近 150 個，包括以下網域名稱：

- claim32200-for2021-taxcredit[.]com

- com-irs[.]xin
- federaltaxrebate-programs[.]click
- gov-irs[.]net
- irsagencygov[.]com
- irs-gov[.]space
- irs-government[.]com
- tax-accounting-services-1801[.]click
- tax-calculator-31430[.]bond
- taxhelp-securelink[.]com
- taxirs-gov[.]com

下圖顯示 2025 年元月每天新註冊的可疑美國國稅局 (IRS) 或稅務主題的不規矩網域名稱之情況。



賽門鐵克可保護您遠離這些威脅，其識別方式如下：

- 所有啟用 WebPulse 的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。

2025/02/18

Vgod勒索軟體

Vgod 是最近在真實網路情境上發現的全新勒索軟體。檔案被加密後，惡意軟體會在加密檔案中冠上 .vgod 副檔名。勒索 (贖金支付) 通知會以一個名為「Decryption Instructions.txt」的文字檔形式出現，攻擊者會要求受害者與他們聯絡以取得解密指示。Vgod 勒索軟體還會更改受感染機器的桌面背景，向受害者提示檔案已被加密。

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)：

- SONAR.Ransomware!g1
- SONAR.Ransomware!g7

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.A!300
- Heur.AdvML.B
- 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**。