保安資訊--本周(台灣時間2025/04/18)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 35 萬 9,700 台受保護端點上總共阻止了 4,660 萬次攻擊。這些攻擊中有 83.7% 在感染階段前就被有效阻止：**(2025/04/14)**

- 在**7萬6,600**台端點上，阻止了**1,780**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**610**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬3,400**台**Windows**伺服主機上，阻止了**700**萬次攻擊。
- 在**4萬7,000**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬500**台端點上，阻止了**69萬2,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,300**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**10萬300**台端點上，阻止了**230**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,100**台端點上，阻止了**74萬7,900**次加密貨幣挖礦攻擊。
- 在**10萬6,400**台端點上，阻止了**690**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**531**台端點上，阻止**7**萬次加密勒索嘗試。

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 18 萬 700 個受保護端點上阻止了總計 750 萬次攻擊。**(2025/04/14)**

- 使用網頁信譽情資，在 **173.6K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **19.9K** 個端點上 **288.9K** 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 **5.7K** 個端點上攔截 **109.4K** 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 **226** 個端點上攔截 **2.1K** 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。

2025/04/17

駭客組織Shuckworm正在大肆散布PteroLNK惡意軟體

PteroLNK 是最近在真實網路情境裡經常發現源於 Pterodo 惡意軟體的最新變種，屬於進階持續威脅 (APT) 的駭客組織 Shuckworm(亦稱 Gamaredon)。該惡意軟體以混淆的 VBScript 形式出現，其中包含惡意程式下載器和利用 .LNK 捷徑檔的植入器元件。部署惡意程式下載器目的是執行從攻擊者控制的 C&C 伺服器擷取其他任意有效酬載。.LNK 捷徑檔的植入器元件則負責管理惡意軟體在受感染網路中的傳播，其方式是取代合法檔案並植入導致進一步感染的惡意捷徑。

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：

- ISB.Malscript!gen26
- 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。

2025/04/17

進階持續威脅(APT)的駭客組織：Fritillary進行中的網路攻擊行動

一起針對歐洲外交單位的全新惡意攻擊行動據悉是由進階持續威脅 (APT) 的駭客組織：Fritillary(亦稱 Midnight Blizzard、APT29) 所發起。根據 Checkpoint 最近研究，攻擊者一直在利用全新自訂惡意軟體載入程式 GrapeLoader 以及 WineLoader 後門的後繼新變種。此行動的主要目的可能是偵查和傳送可能用於後續攻擊階段後門程式的二進位檔案。

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：

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

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。

2025/04/17

全新的無檔案型態惡意軟體網路攻擊行動，最終會注入XWorm遠端存取木馬以及Rhadamanthys惡意竊密程式

新的惡意軟體攻擊活動使用 JScript 和混淆的 PowerShell 指令來部署，例如：XWorm 遠端存取木馬和 Rhadamanthys 惡意竊密程式等高度迴避性的惡意軟體。此網路攻擊行動針對 Windows 系統，利用工作排程或幾可亂真網頁或文件外觀 (ClickFix) 搭配假冒的圖靈 (CAPTCHA) 驗證機制，誘騙使用者執行惡意有效酬載。惡意軟體利用無檔技術進行傳播，目的是入侵系統以進行監控、擷取敏感資料或賺取非法金錢。

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.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2025/04/16

DragonForce勒索軟體的攻勢在2025年變本加厲

在 2024 年，DragonForce 勒索軟體涉入的攻擊行動非常活躍，在其洩密網站上聲稱約有 93 名受害者，可能還有更多受害者未被揭露。現在還算是 2025 年初，該駭客組織就誇口有 40 多家跨國跨領域的組織也即將成為它們的囊中物。

- 國家：美國、義大利、英國、埃及、法國、德國、中國、新加坡、紐西蘭、沙烏地阿拉伯、澳洲、挪威、捷克共和國、丹麥、印尼
- 行業：電信、紡織品製造、法律與會計服務、電子與 IT 服務、鋼鐵與金屬製造、諮詢與工程服務、汽車業、醫療保健、運輸與物流、能源與環境服務、航空電子與工業製造、建築、建材、消費品製造、保險與房地產、科技與 GIS 服務、市政服務

電腦一旦遭受攻擊成功，被加密的檔案會冠上 .dragonforce_encrypted 或 .cyberbears 副檔名。他們的贖金說明宣稱檔案被竊取和加密，並表示該組織是出於經濟目的而非政治目的。受害者會被指示透過 Tor 加密網站或 TOX ID 與攻擊者聯絡，以取得被盜檔案的清單，然後免費解密一個檔案以證明其工具有效。

還警告被害者，如果未在指定日期前聯繫，被竊資料將會在該組織的洩密網站上被公開。說明的結尾是一個二進位字串，拼成「DragonForce」。該組織還聲明，只要付款，他們就會刪

除竊取的資料、提供解密程式，並提供一份關於資料外洩的報告與安全建議。

在先前攻擊和最近報告中，已觀察到此主使者利用 PowerShell 和 WMIC 等就地取材的兩用工具 (LOLBins) 進行初始執行和隱匿。他們使用 Cobalt Strike、Mimikatz 和 SoftPerfect Network Scanner 等網路滲透測試工具進行後續攻擊，以實現橫向移動、憑證竊取和內部偵察。為了規避安全軟體的偵測，他們會使用以自帶含有漏洞的驅動程式」(bring-your-own-vulnerable-driver，簡稱 BYOVD) 和清除事件日誌等伎倆來阻礙偵測和回應。

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.DragonForce
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/04/16

Agent Tesla惡意程式涉入近期的多階段攻擊行動

如今，惡意垃圾郵件已成為常態而非例外。透過惡意附件傳送多階段攻擊已成為常態。Palo Alto Networks 的研究人員發表一份報告，分享使用 Agent Tesla 惡意程式作為最終有效酬載的攻擊行動的詳細資訊。

此攻擊始於傳送壓縮檔附件的社交工程電子郵件。該檔案包含一個惡意 JS 檔案，可啟動感染鏈。這個腳本會以 PowerShell 腳本的形式下載下一個階段。PowerShell 指令碼會被注入並執行最後的可執行有效酬載，這些有效酬載會被載入記憶體，然後再注入合法的程序。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2
- ACM.Ps-Wscr!g1
- ACM.Rgsvc-Lnch!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g532
- SONAR.SuspOpen!gen11

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!gen60
- ISB.Downloader!gen68
- ISB.Dropper!gen1
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malautoit!g3

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: Scripting Host Processes Making Network Connections
- Audit: Suspicious Process Accessing Lets Encrypt Certified Site

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。

2025/04/16

針對微軟Visual Studio Code(VSCode)用戶的攻擊行動，駭客利用惡意VSCode擴充套件來散佈惡意挖礦程式

在新一波惡意挖礦程式散佈行動中，觀察到駭客冒充合法開發工具利用惡意 VSCode 擴充套件來散佈惡意挖礦程式。當這些惡意的 VSCode 擴充套件被安裝和啟動時，它們會從外部來源取得 PowerShell 腳本並執行它。PowerShell 腳本會執行多種功能，例如：停用安全軟體、建立持久性、提升權限，以及最終載惡意挖礦程式。腳本完成後，惡意擴充套件會採取額外的步驟來安裝它所冒充的合法擴充套件，以便使用者不會察覺感染。

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.Ps-Reg!g1
- ACM.Ps-Schtsk!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!g1
- ACM.Ps-CPE!g2

- ACM.Untrst-RunSys!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：

- PUA.Gen.2
- Trojan.Gen.MBT
- Trojan.IcedID
- Web.Reputation.3
- WS.Malware.1
- 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
- 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。

2025/04/16

DOGE BIG BALLS勒索軟體

據報導，一起全新的勒索軟體攻擊行動利用美國政府效率部 (Department of Government Efficiency，簡稱 DOGE) 內一位知名人士的名字來欺騙受害者。涉入該攻擊行動的被稱為「DOGE BIG BALLS」，源於 Fog 勒索軟體的後繼新變種。

此攻擊始於使用者被包含捷徑檔 (.LNK) 金融主題的 ZIP 壓縮檔案所引誘。開啟這些檔案後，會觸發一個多階段 PowerShell 腳本檔，以建立持久性、滲透敏感的系統資料，並傳送自訂有效酬載，包括一個核心模式攻擊工具。該攻擊工具利用 10 年前的 Intel 驅動程式漏洞 (CVE-2015-2291) 以自帶含有漏洞的驅動程式」(bring-your-own-vulnerable-driver，簡稱 BYOVD) 技術，允許攻擊者取得勒索軟體程序所需的核心層級讀／寫存取權限以及權限提升。

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-Http!g2
- ACM.Ps-Net!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomFog!g1
- SONAR.Ransom!gen112
- SONAR.Ransomware!g16
- SONAR.SuspDriver!g10
- SONAR.SuspDriver!g26

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!aat171
- Ransom.Fog
- Scr.Mallnk!gen13
- Trojan.Gen.MBT
- Web.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

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。

2025/04/15
防護亮點：有效應對好工具拿來幹壞事的灰色地帶～雲端Web表單武器化的網路釣魚攻擊

網路釣魚行動持續演進，手法也層出不窮，利用合法的雲端工具繞過安全控制並取得使用者信任。在這些工具中，NoCodeForm 和 Submit-Form 已成為攻擊者利用的便捷網路表單服務，用於收集憑據和其他敏感資訊。本文探討這些服務在網路釣魚攻擊中的使用方式，並提供保護解決方案。

什麼是 NoCodeForm 和 Submit-Form

NoCodeForm

NoCodeForm 是一種雲端、無程式碼的網路表單服務，可讓使用者在不需要具備任何程式設計能力的情況下快速建立和部署網路表單。它被廣泛用於問卷調查、客戶回涵和資料收集。該平台支援各種應用情境的高度整合，包括電子郵件通知、webhooks 和 API 。一旦遭到濫用於自動化的資料滲透，危害程度勢必非同小可。

Submit-Form

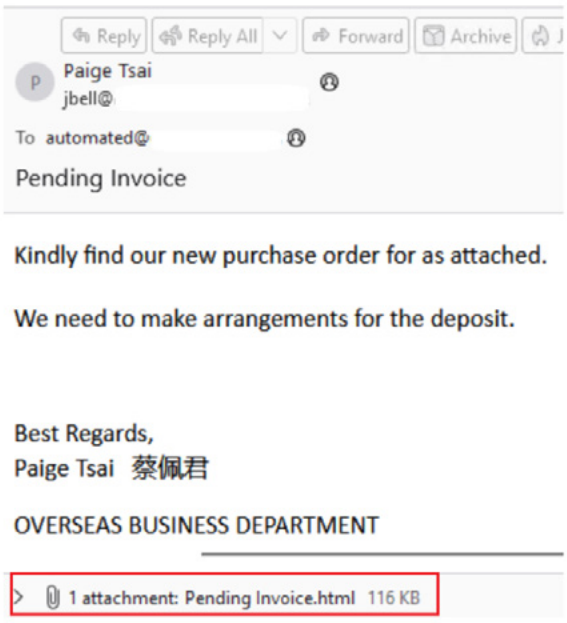
Submit-Form 也是一項類似的服務，可讓使用者透過簡單的 HTML 整合，收集並儲存表單提交內容。它通常用於聯絡表單、註冊頁面和線上回應機制。攻擊者可利用其匿名表單提交功能和資料轉發選項，將竊取的憑證重導向至外部伺服器。

這兩種服務都提供易用和無縫整合，因此對合法使用者和網路罪犯都很有吸引力。

攻擊者如何在網路釣魚活動中濫用這些服務

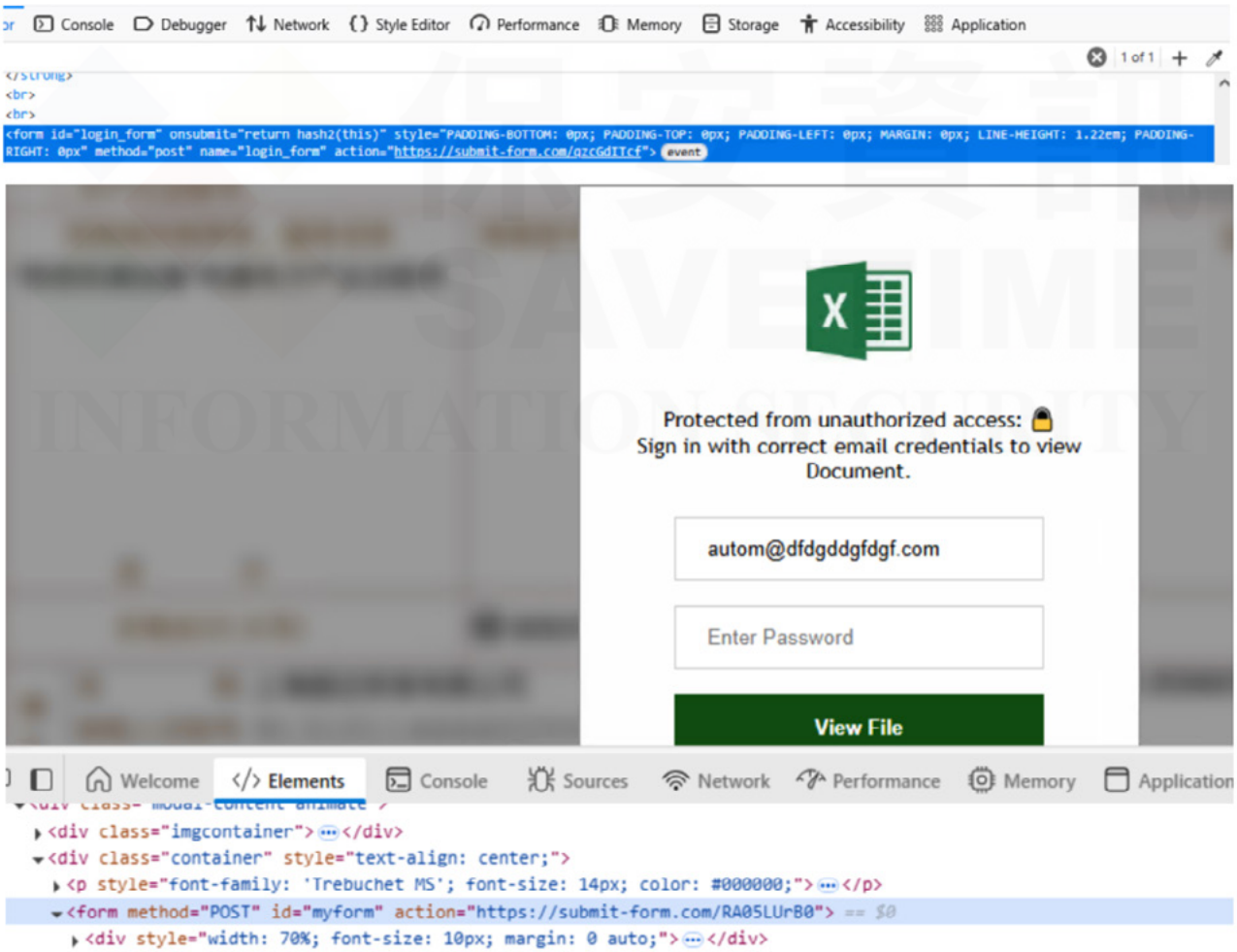
1. 建立惡意表單

攻擊者使用表單建立程式介面仿造複製登入頁面。這些網頁通常會模仿合法的服務 (例如：Microsoft 365、Google 或銀行入口網站)。表單的動作網頁設定為攻擊者控制的端點，或使用內建的提交儲存，以便稍後擷取。



2.將表單上架在可信賴的網站

由於這些服務為表單式互動提供寄存／上架服務，攻擊者會利用其合法性來逃避安全掃描。由 NoCodeForm 和 Submit-Form 所產生的網頁通常會繼承該平台的可信任度，因此不太可能被自動安全工具所標記。



3.竊取蒐集到的資料

Webhook 類型的資料滲出：攻擊者設定 Webhooks，以即時將擷取的憑證自動傳送至遠端伺服器。

濫用 API 整合能力：某些服務允許與 API 整合來進行資料擷取，讓攻擊者能以程式化的方式存取所竊取的憑證，而無需手動介入。

濫用電子郵件轉寄：許多雲端表單服務提供新提交的電子郵件通知，可用於將竊取的憑證悄悄轉發至攻擊者控制的電子郵件帳戶。

4.繞過傳統安全防護機制

傳統安全機制 (例如：網域信譽分析和網頁過濾) 可能無法標示這些網路釣魚嘗試，因為這些表單是上架在知名、有信譽的網站上。這使得它們可以有效地躲避自動化的安全工具。此外，有些攻擊者會使用短網址服務或重導向服務來混淆網址，以進一步逃避偵測。

賽門鐵克的郵件防護方案：滿足雲端服務與地端自建的需求

Symantec Email Security.cloud

Symantec Email Security.cloud 是賽門鐵克郵件安全雲端服務，可同時保護雲端電子郵件平台 (例如：Office 365、Google Workspace) 和內部部署的系統 (例如：Microsoft Exchange)。利用多層次防禦，它可以阻擋勒索軟體、魚叉式網路釣魚和商務詐騙 (BEC) 等進階威脅，同時透過進階分析和與賽門鐵克全球威脅情資網路 (GIN) 的整合，提升攻擊活動的能見度。

- 惡意軟體與垃圾郵件防禦：採用信譽分析、防毒引擎和反垃圾郵件特徵來檢查連結和附件。
- 連線層級 (IP 層級) 防護：透過降低異常 SMTP 連線的速度和丟棄，以降低垃圾郵件和惡意軟體的風險。
- Click Time & Link Following (即時鏈接檢)」：在電子郵件傳送前即時掃描，並在點擊時再次掃描，追蹤連結至其最終目的地。
- 電子郵件威脅隔離：以唯讀模式開啟有風險或未知的網站連結或附件，保護使用者免受網路釣魚攻擊。
- 模仿控制：透過複雜的模仿引擎防止商務郵件詐騙 (BEC) 和偽造，以阻止模仿合法使用者或網域的威脅。
- 資料隱私規範：內部 DLP 及加密政策與規則可保護訊息或附件中的公司資料。

Symantec Messaging Gateway

Symantec Messaging Gateway 是一套地端自建的電子郵件安全解決方案，可針對最新的訊息傳輸威脅提供入埠和離埠防護，包括勒索軟體、魚叉式網路釣魚和商業電子郵件入侵 (BEC)。它能攔截 99% 以上的垃圾郵件，並提供內建的資料保護功能，以確保電子郵件的安全和機密性，而且還能透過即時的反垃圾郵件和反惡意軟體威脅情報，有效回應新的訊息傳輸威脅。

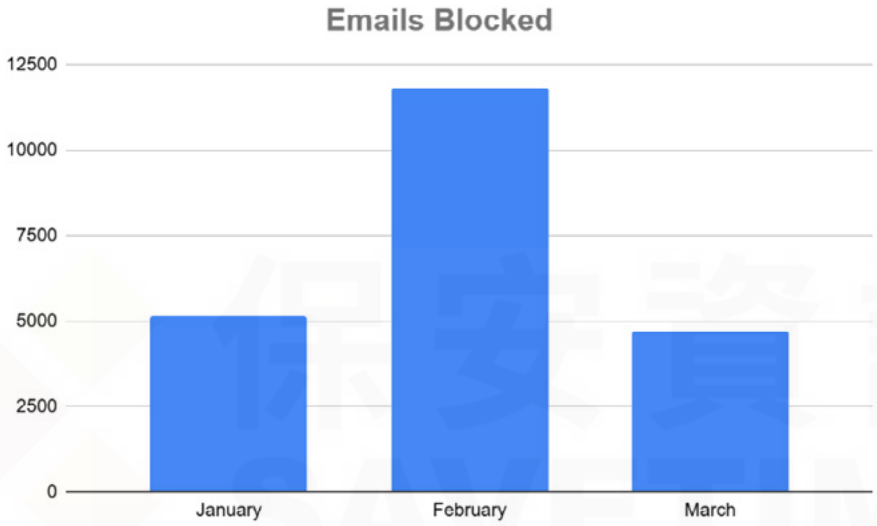
- 保護敏感資料：內部 DLP 政策可保護訊息或附件中的公司資料，防止其離開機構。
- 阻止進階威脅：多層偵測技術可攔截可疑電子郵件，以防禦網路釣魚、勒索軟體和 BEC 攻擊。
- 阻止不需要的電子郵件：內容過濾可防止傳送含有惡意連結和附件的電子郵件，這些惡意連結和附件會用來傳送垃圾郵件和惡意軟體。

賽門鐵克的反垃圾郵件 (Anti-Spam) 過濾系統

預測性過濾系統專注於攻擊媒介的不同屬性，並適時部署其他電子郵件功能，以捕捉快速演變的電子郵件威脅形勢的變化。在預測性過濾系統的支援下，以電子郵件為媒介的威脅會在造成損害之前被過濾和阻擋。這種方法在協助偵測這些類型攻擊的頻繁變化方面，也證明是富有成效的。

賽門鐵克的反垃圾郵件 (Anti-Spam) 過濾系統攔截的電子郵件

以下圖表顯示賽門鐵克的反垃圾郵件 (Anti-Spam) 過濾系統 (~21K) 在 2025 年 1 月到 3 月間攔截到這類型的惡意垃圾郵件。



NoCodeForm 和 Submit-Form 提供合法的雲端網頁表單解決方案，但它們在網路釣魚活動中遭濫用，突顯出需要更強大的偵測和緩解策略。網路安全專業人員必須利用威脅情報、行為分析和主動安全政策來有效對抗這些威脅，以保持領先地位。透過瞭解這些服務如何被利用，組織可以更有效地保護使用者免於複雜的網路釣魚攻擊，同時仍允許合法使用這些雲端生產力工具。

欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲深入瞭解更多有關 Symantec Messaging Gateway 的資訊，請點擊此處。

2025/04/15

Linux平台上的BPFDoor後門程式，涉入近期在亞洲和中東的攻擊活動

Linux 平台上的 BPFDoor 後門程式，在針對亞洲和中東各產業的攻擊中被發現。該惡意軟體因使用 Berkeley Packet Filtering 而得名，可根據網路封包檢測過程中發現的特定序列來啟動過濾器功能。惡意程式會開啟一個反向 shell，讓攻擊者進一步進入被攻擊的網路，暴露其他系統和敏感資料。

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：

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.BPFDoor
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

2025/04/15

CVE-2025-30208--存在Vite的任意檔案讀取漏洞

Vite 是一個前端開發和打包工具，致力在提供快速和高效的開發體驗。CVE-2025-30208 是近期被揭露存在 Vite 的任意檔案讀取漏洞。如果被成功開採濫用，該漏洞可能會允許未經認證的攻擊者繞過路徑存取限制，並授予他們任意檔案讀取權限。原廠已在 6.2.3、6.1.2、6.0.12、5.4.15 及 4.5.10 版本修補此漏洞。

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: Vite CVE-2025-30208

2025/04/14

勸世文：色字頭上一把刀，石榴裙下命難逃～安卓平台的熱門惡意程式：SpyNote，藏身在假冒的盜版情色成人網站手機APP裡

色情一直以來就是最有效的社交工程伎倆之一，原因在於高好奇心驅使的參與程度、阻礙受害者舉報的污名，以及可透過行動式攻擊 (例如：偽造 APK) 輕易將其武器化。世界各地的威脅份子持續利用成人主題來傳送惡意軟體、竊取憑證和發起色情勒索詐騙，通常會將其活動嵌入假冒的成人視訊 (AV) 或約會應用程式 (APP) 中。

在最近一個案例中，我們觀察到威脅份子利用偽造的 MissAV 行動 APP 誘騙受害者，冒充在日本和韓國擁有龐大使用族群的影音串流平台。該惡意安卓平台 APP 上架在一個幾可亂真的假冒網站，利用拚字錯誤的域名手法 (typosquatting) 來誤導毫無戒心的受害者，該網域經過精心設計，與合法網站十分相似，誘騙使用者下載惡意軟體。此行動似乎是在今年初原版 MissAV 平台因涉嫌侵權而被查封之後發生的--促使使用者轉而搜尋其他存取點，不慎將他們引導至幾可

亂真的假冒網站。

這個偽造的 APP 就是大名鼎鼎的 SpyNote，是一個遠端存取的木馬程式，能夠錄音、擷取螢幕截圖、收集簡訊和通話記錄，並遠端控制裝置。對消費者而言，這會導致嚴重的隱私侵犯、身分盜用，甚至勒索，特別是引誘性的成人主題性質。對於企業使用者而言，風險更大--SpyNote 可以存取企業資訊。在這種情況下，攻擊者可能會利用個人和企業資料進行更嚴重的勒索，威脅洩露敏感的企業資訊，同時洩露個人內容。

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。

- Spyware:MobileSpy

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。

2025/04/14

網路釣客冒充土耳其職業介紹所，散布夾帶「Snake」鍵盤側錄器的惡意郵件

賽門鐵克最近觀察到一起「Snake」鍵盤側錄器攝入的網路攻擊行動，目標是土耳其的機構組織，包括航太與國防及金融服務業。

初始攻擊是一個經過精心製作，看起來像是來自土耳其國家就業機構 İŞKUR 的官方通訊的偽造郵件。該郵件聲稱在公司稽核期間發現違規行為，並敦促收件者在三個工作天內提交經簽署的書面反對意見。

- 電子郵件主旨： Denetim kurulu raporu {ŞİRKETİNİZİN SİCİL DENETİMİ}
- 翻譯： 稽核管理報告 {貴公司的登記稽核報告}

該電子郵件的附件是一個 .RAR 壓縮檔 (ISKUR Denetim kurulu raporu No 2025-GE-218567.rar)，其中包含「Snake」的鍵盤側錄器，這是專門用來竊取敏感資訊，例如：按鍵、憑證、剪貼簿資料和螢幕截圖，並能夠透過 SMTP、FTP 或 Telegram 外洩資料。

除了上述行為之外，最近觀察到新變種還運用多種 MITRE ATT&CK 框架中的各種 TTPs：戰術 (Tactic)、技術 (Technique)跟程序 (Procedure)。這些 TTPs 包括透過指令和腳本編釋器執行、DLL 側載和程序注入以達到持久性／常駐能力和權限升級／提權，以及使用混淆、打包和隱藏物件以試圖迴避安全軟體偵測。

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：

- Packed.Generic.635
- Trojan.SnakeKeylogger
- Scr.Malcode!gdn34

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：

- Audit: TLS v1 Request
- Audit: Untrusted Telegram API Connection

2025/04/15

ZeroTrace(*零追蹤)惡意竊密程式

ZeroTrace 是一款全新的惡意竊密程式，最近在威脅生態圈嶄露頭角。此惡意軟體的自動產生器透過各種地下論壇和檔案分享平台散佈，並宣稱僅用於教育和研究目的。ZeroTrace 是採用 C# 所撰寫，具有從受感染的機器中滲出各種機密資料之功能。目標資料包括憑證、加密貨幣錢包、cookie、瀏覽器歷史紀錄、使用者檔案、Discord 和 Telegram 資料等。收集到的資訊可能會在 Discord 或 Telegram 的協助下回傳給攻擊者。

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

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
- WS.Malware.1

基於機器學習的防禦技術：

- 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
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 654
- System Infected: Trojan.Backdoor Activity 721

2025/04/14

Pulsar遠端存取木馬(RAT)

Pulsar 是最近在真實網路情境裡發現的全新遠端存取木馬 (RAT)。這個採用 C# 撰寫的惡意軟體是源於 Quasar 遠端存取木馬 (RAT) 的進化版本，具有多種功能，包括鍵盤側錄、加密貨幣錢包剪貼簿劫持、資料竊取、檔案管理、遠端 shell 和指令執行等。此惡意軟體的資料竊取功能包括收集和滲出敏感資訊，例如：憑證、cookie、加密錢包、會話檔案和儲存在系統網路瀏覽器中的資料等。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen57

- SONAR.SuspBeh!gen93
- SONAR.SuspBeh!gen609
- SONAR.SuspBeh!gen752
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan.Gen.MBT
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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
- System Infected: Bad Reputation Application Connecting to Cloud Storage
- System Infected: Trojan.Backdoor Activity 721

2025/04/14

假仁慈？還是盜亦有道？PelDox勒索軟體只加密，保證不會洩露你的資料

與典型的勒索軟體不同，PelDox 不會通知受害者其檔案已被加密，也不會要求支付解密費用。在加密檔案並冠上「.lczx」副檔名之後，勒索軟體會顯示一則全螢幕訊息。此訊息偽稱網路罪犯已保護受害者的檔案不會「被竊或洩漏」。然後，它建議受害者考慮寄送金錢，以表達對此項「服務」的感謝，並提供 Telegram 聯絡人，以便進一步溝通。

付款後，受害者會收到如何復原檔案和移除惡意軟體的指示。訊息還警告受害者不要關閉電腦，因為這樣做可能會進一步損壞加密的檔案。

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：

自適應防護技術(包含於SESC)：

- ACM.Mshta-Ps!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-THta!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：

- Downloader
- ISB.Downloader!gen77
- ISB.Downloader!gen205
- ISB.Downloader!gen221
- Packed.Generic.143
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2025/04/13

HijackLoader新增隱身和迴避的新模組

HijackLoader (又稱為 GHOSTPULSE 或 IDAT Loader) 是一個惡意軟體載入器，能夠提供攻擊鏈的第二階段有效酬載，並提供多種模組，主要用於設定資訊、安全軟體的規避，以及程式碼的注入／執行。模組化架構允許透過新模組持續更新功能。最近在 HijackLoader 的武器庫中發佈的新模組包括用於掩蓋函數呼叫來源的呼叫堆疊欺騙、用於檢測分析環境的反虛擬 (虛擬感知) 檢查，以及透過工作排程的常駐能力。

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：

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：

- Trojan.Gen.MBT
- Trojan Horse
- W32.Fixflo.B!inf
- 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。

2025/04/11

NanoCrypt勒索軟體～開發過程類似群眾外包的概念

NanoCrypt 是在真實網路情境裡發現另一種「普通」勒索軟體。此惡意軟體會加密使用者資料，並冠上 .ncrypt 的副檔名。以檔名為 README.txt 文字檔形式釋出的勒索贖金支付說明指出，此惡意軟體是「為了好玩」而製作，並非用於任何有害活動。雖然惡意目的可能並非其創造者的本意，但類似的「測試」勒索軟體經常被威脅者採用和修改，以便在真正的攻擊中進一步散佈。

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

於行為偵測技術(SONAR)的防護：

- SONAR.RansomGen!gen5
- SONAR.Ransomware!g34

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

- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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**。