保安資訊--本周(台灣時間2025/04/25)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 34 萬 1,200 台受保護端點上總共阻止了 5,200 萬次攻擊。這些攻擊中有 83.7% 在感染階段前就被有效阻止：**(2025/04/21)**

- 在**7萬9,000**台端點上，阻止了**2,200**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬3,500**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**2萬3,100**台**Windows**伺服主機上，阻止了**640**萬次攻擊。
- 在**4萬8,600**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,700**台端點上，阻止了**10**萬次嘗試掃描在**CMS**漏洞。
- 在**4萬5,500**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**9萬1,200**台端點上，阻止了**210**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**65萬9,000**次加密貨幣挖礦攻擊。
- 在**9萬7,800**台端點上，阻止了**690**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**558**台端點上，阻止了**7萬8,000**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 15 萬 7,300 個受保護端點上阻止了總計 650 萬次攻擊。**(2025/04/21)**

- 使用網頁信譽情資，在 **150.8K** 個端點上阻止 **610** 萬次攻擊。
- 攔截 **18.4K** 個端點上 **285.7K** 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 **5.2K** 個端點上攔截 **126.9K** 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 **272** 個端點上攔截 **2.5K** 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。

2025/04/24

出現偽造日本農林中央金庫(Norinchukin Bank)登入頁面的網路釣魚活行動～存戶請小心

Norinchukin (Nochu) Bank 成立於 1923 年，是一家支援農業部門的日本合作銀行。它是農業合作社集團 JA Bank 的全國性機構。最近，賽門鐵克偵測到針對該銀行線上金融服務存戶的網路釣魚行動。這些詐騙電子郵件冒充銀行，傳送虛假的帳戶通知，並促請收件者點擊連結確認帳戶詳細資料。此連結會將使用者重導向至偽造的登入頁面，目的是竊取他們的憑證。一旦做入圈套，攻擊者就可以登入受害者的帳戶。

電子郵件標題：

- 【重要なお知らせ】[JAネットバンク]お客さま情報等の確認について。
- 翻譯：[重要通知] [JA Net Bank] 關於確認客戶資料等。

維基百科知識：農林中央金庫 Norinchukin 銀行，也稱為 Nochu 銀行，是一家日本合作銀行，總部位於東京，為超過 5,612 個農業、漁業和林業合作社提供服務。Nochu 是日本最大的機構投資者之一，投資組合超過 4,000 億美元，資產超過 8,400 億美元。

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：

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)。

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。

2025/04/23

PE32勒索軟體～看起來不怎麼樣， 但仍對資安意識薄弱與防護不周的系統構成重大威脅

PE32 是新發現的勒索軟體，利用 Telegram 進行 C&C 作業。它採用雙重勒索模式，對檔案解密和資料保密分別收取費用。儘管它的程式碼雜亂、簡單，而且使用基本的 Windows 函式庫，但仍對資安意識薄弱與防護不周的系統構成重大威脅。

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.MalTraffic!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：

- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.MBT

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

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 564
- System Infected: Trojan.Backdoor Activity 654

2025/04/23

駭客利用Proton66防彈主機服務擴大惡意程式與控制與命令(C&C)的攻擊能量

Proton66 防彈主機服務已成為惡意網路活動的中心樞紐，提供用於網路攻擊的 C&C 作業和網路釣魚行動的基礎架構，常見的 GootLoader、SpyNote 和 XWorm 等惡意軟體的散佈行動也常藉助這個基礎架構。最近攻擊包括遭攻擊的 WordPress 網站將 Android 使用者重導向至偽造的 Google Play 商店頁面，以及公開曝光的 ZIP 檔案，其中包含韓語使用者的個人資料和 XWorm 有效酬載。該基礎架構也與 WeaXor 勒索軟體有關聯，WeaXor 是一種全新的 Mallox 後繼新變種，會在被加密的檔案冠上「.wex」副檔名。

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
- ACM.Untrst-FlPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!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!aat171
- ISB.Downloader!gen285
- ISB.Downloader!gen544
- ISB.Heuristic!gen62
- Scr.Malcode!gen
- 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: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 568

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。

2025/04/23

初始入侵管道掮客(IAB)：ToyMaker為Cactus勒索軟體的攻擊行動開路

初始入侵管道掮客或稱初始存取掮客 (IAB) 通常是威脅份子成功發動攻擊的第一步。IAB入侵後會收集憑證相關資料，然後將這些資訊出售給威脅份子，為接手從事攻擊行動的駭客，提供存取目標網路環境的進一步入侵能力。Cisco Talos 的研究人員報告一個名為 ToyMaker 的 IAB，並提供他們稱為 LAGTOY 的客製化植入程式的技術細節。該報告也分享 ToyMaker 向發動 Cactus 勒索軟體攻擊駭客提供存取權限的幾個特定活動的詳細資訊。

網路知識：初始入侵管道掮客或稱初始存取掮客 (Initial Access Broker：IAB)，就是專門收集可存取特定組織帳密資料的角色，可以想像為專門竊取大門鎖匙賣給小偷的人，如果重要 IT 基礎架構的帳密被竊且轉賣給駭客，就如同門戶大開完全沒有門禁，任何的防護措施也都沒用。

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：

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.Trojan
- Meterpreter
- Packed.Generic.347
- Packed.Generic.539
- Trojan Horse
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.A!300

- 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。

2025/04/23

遭惡意篡改過的Alpine Quest APP，被用來透過Telegram Bot監視俄羅斯軍方

受歡迎的 Android 導航應用程式 (APP)：Alpine Quest 出現被篡改過版本被發現含有針對俄羅斯軍方人員的間諜軟體。附身在該 APP 中的間諜軟體會收集敏感資訊，例如：電話號碼、帳戶資訊、聯絡人和地理位置。這些資料會傳送到攻擊者控制的遠端伺服器和 Telegram 殭屍，每次使用者移動時，位置資訊都會更新。攻擊者似乎特別關注透過 Telegram 和 WhatsApp 等通訊軟體分享的文件。

網路知識：

- AlpineQuest 是所有戶外活動和體育運動的完整解決方案，包括遠足、跑步、尋寶、狩獵、航海、地理作業、越野導航等等。
- Telegram 是通訊軟體，也可自行開發程序，好的用途可以做個像 Line 機器人一樣的功能，故用來當系統運行 Fail 時的通知，也可能淪為壞人的犯案工具。

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。

2025/04/23

近期在真實網路情境裡發現的FormBook惡意竊密程式散佈行動

Fortinet 研究人員報告一起全新 FormBook 惡意竊密程式散佈行動。攻擊者濫用內含 CVE-2017-11882 陳年老漏洞的惡意 Word 文件進行攻擊，CVE-2017-11882 是早在 2017 年就存在 Microsoft Office Equation Editor 漏洞。成功濫用此漏洞可能會讓攻擊者在受感染的機器上執行有效酬載傳送和遠端程式碼執行。涉入此攻擊行動中有效酬載是以 .png 檔案的形式傳送，該檔案之後會解密為 Formbook 可執行二進位檔。Formbook 是一種在駭客圈備受推崇且非常盛行的惡意竊密程式，多年來一直是威脅生態圈的要角，全球各地的各種駭客組織與個體戶都在使用。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Rd32-RgPst!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。

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：

- Bloodhound.RTF.10
- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Bloodhound.RTF.25
- Exp.CVE-2017-11882!g2
- Exp.CVE-2017-11882!g3
- Exp.CVE-2017-11882!g5
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.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!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。

2025/04/23

進階持續威脅(APT)駭客集團：Billbug持續在東南亞發動網路攻擊行動

進階持續威脅 (APT) 駭客集團：Billbug (又名 Lotus Blossom、Lotus Panda、Bronze Elgin) 在 2024 年 8 月至 2025 年 2 月入侵行動中，入侵東南亞國家的多個組織。目標包括政府部門、航空交通管制單位、電信商和建設公司。除此之外，該駭客集團還對位於東南亞另一個國家的新聞機構和位於另一個鄰近國家的航空貨運公司發動入侵攻擊。這些攻擊涉及使用多種新的自訂工具，包括惡意程式載入器、憑證竊取器和反向 SSH 工具。

請參閱我們的部落格文章：進階持續威脅 (APT) 駭客集團：Billbug 持續在東南亞發動網路攻擊行動。

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.Sagerunex
- ChromeKatz
- CredentialKatz
- Hacktool.Rexershell
- Trojan Horse
- WS.Malware.1
- WS.Reputation.1
- WS.SecurityRisk.3

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
- Heur.AdvML.C

2025/04/22

濫用未修補漏洞的TOTOLINK裝置，RustoBot殭屍網路攻擊大爆發

RustoBot 是一種採用 Rust 語言撰寫的全新殭屍網路，透過濫用未修補 TOTOLINK 裝置的漏洞散佈。根據 Fortinet 最新報告，此惡意軟體已在最近攻擊行動中散佈，目標為各種架構，包括 x86、arm5、arm6、arm7、mips 和 mpsl。RustoBot 惡意軟體主要功能是從受攻擊的裝置發動分散式阻斷服務 (DDoS) 攻擊。

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：

- CL.Downloader!gen277
- Linux.Mirai
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2025/04/22

防護亮點：憑證轉存(Credential Dumping)的危害--有效滲入企業網路和促進橫向移動的入口

取得目標組織的憑證是攻擊者為了達成各種目的的首要目標。這是攻擊初始階段之一，作為滲入企業網路和促進橫向移動的入口。憑證可從各種來源取得，包括作業系統和第三方工具。多個地下論壇會向駭客組織提供／兜售憑證，有些行動者會使用新穎的方法來取得這些憑證。遭竊取的憑證通常以雜湊 (hash) 或明文傳輸密碼的形式存在。

攻擊者使用作業系統憑證轉存手法

取得帳戶登入資訊和憑證，對於攻擊者的攻擊活動至關重要，因為這可讓他們

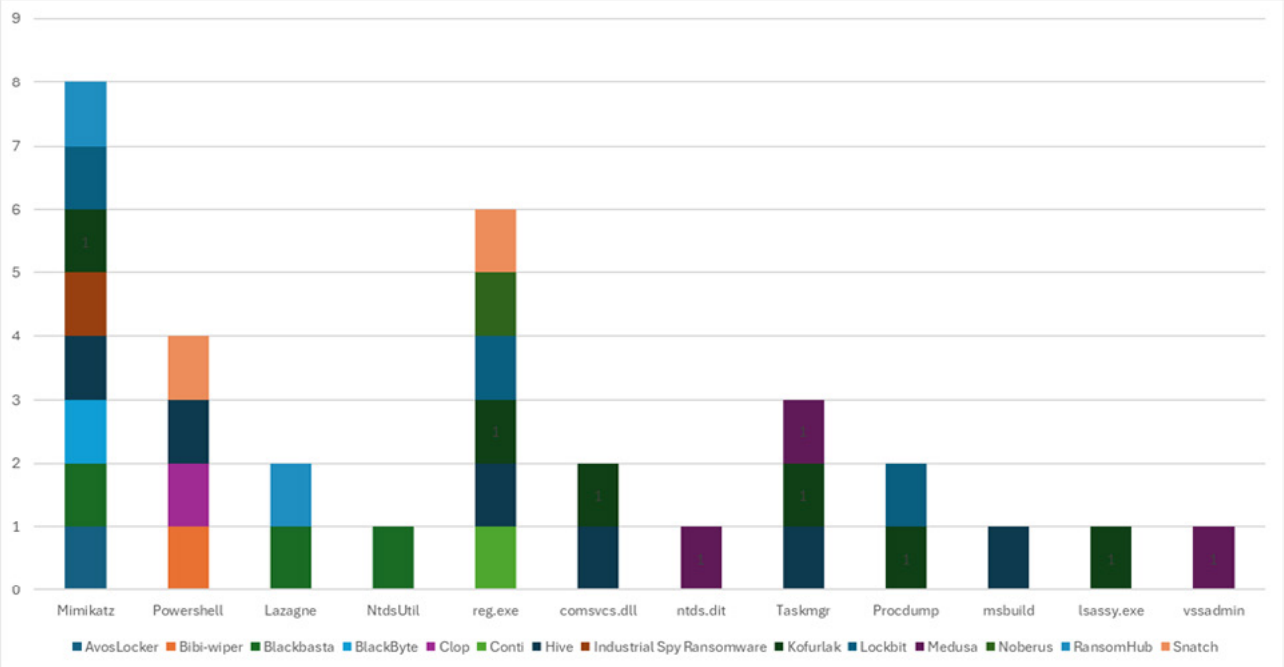
- 存取受限制的資訊、網路資源和重要資產
- 以新的權限存取網路內的其他系統和服務
- 建立新帳號並將其刪除，滅跡以阻礙鑑識分析
- 透過密碼模式和政策收集其他憑證

在 Windows 作業系統中，憑證會儲存在數個地方：

- 安全帳戶管理員(SAM)資料庫
  - Windows Security Accounts Manager(SAM)：是 Windows 用來管理本地用戶帳戶的組件之一。SAM 是一個資料庫檔案，包含以分散式格式儲存的使用者名稱和密碼。
- Windows 本地安全認證子系統服務 (LSASS) 記憶體
  - Local Security Authority Subsystem Service：LSASS 是一個 Windows 程序，負責驗證使用者登入並執行安全政策。當使用者登入時，LSASS 程序會從 SAM 資料庫擷取使用者的憑證，並在會話期間將其儲存在記憶體中。
- NTDS.dit
  - 這是 Microsoft's Active Directory Domain Services 網域服務 (AD DS) 中的主要資料庫檔案。此檔案包含重要的網域資訊，包括使用者的密碼雜湊值。
- Local Security Authority (LSA)本地安全授權隱私
  - LSA 隱私儲存在 HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets 的註冊表中，其中可能包含各種不同的憑證資料。
- 暫存的網域憑證
  - 在網域控制器不可用的情況下，通常儲存在 LSASS 記憶體中的快取網域憑證可用來驗證使用者。
- 憑證管理員
  - Windows Credentials Manager 是一個 Windows 程式，用來儲存認證憑證--主要是網頁和裝置憑證。
- 群組政策(Group Policy)
  - 群組政策允許集中管理 Active Directory (AD) 中的使用者和電腦設定。

常用的憑證轉存工具的使用情境

駭客集團常用的憑證轉存的技術



熱門趨勢

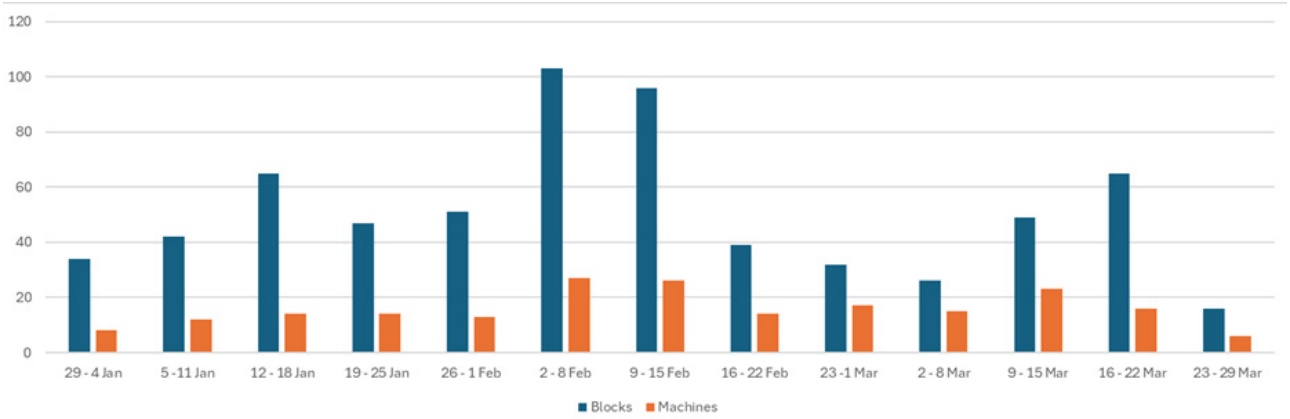
- Mimikatz 是一種開放原始碼的憑證轉存工具，常被駭客利用。最常見 Mimikatz 執行方法包括
  - mimikatz.exe "privilege::debug" "sekurlsa::pth /user: /domain:MEB /ntlm:"
  - mimikatz64.exe "privilege::debug" "log.txt" "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords full"
  - imfa.exe kerberoast /domain:corpmty.ccontrol /outfile:CSIDL_SYSTEM_DRIVE\temp\temp.txt /format:hashcat
- 使用 reg.exe 從 Windows 註冊表轉儲 hive 檔案。這些檔案包含敏感資訊，例如：散列憑證，攻擊者可能會利用這些資訊進行橫向移動。
  - reg save HKLM\SAM sam.hiv
  - reg save HKLM\SYSTEM SYSTEM.hiv
  - reg save HKLM\SECURITY security.hiv
- LaZagne 是一個用於攻擊鏈的入階後階段的開放原始碼工具，用來擷取大量儲存在系統中的密碼。
  - lazagne.exe all > lazagne.txt
- Comsvcs.dll 是合法的 Windows dll，據觀察，駭客會濫用它來轉存程序記憶體，尤其是 LSASS，試圖擷取憑證。
  - rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump <process id> lsass.dmp full
- 使用 Ntdsutil.exe 擷取 Active Directory 資料庫 - NTDS.dit，通常用於離線密碼破解。
  - ntdsutil.exe "ac i ntds" ifm "create full c:\zemp" q q
- Procdump 是一個合法的 Sysinternals 工具，用來產生程序轉存以進行故障排除，但它可能會被駭客用於惡意目的，例如：擷取憑證資料。
  - procdump64.exe" -accepteula -ma <pid> out.dmp
- 使用磁碟區陰影複製 (vssadmin) 從 NTDS 存取憑證資訊。
  - vssadmin create shadow /for=c：

端點偵測與回應(EDR)自動偵測網路中的可疑活動

賽門鐵克端點偵測與回應 (Symantec Endpoint Detection and Response：EDR) 使用機器學習和行為分析來偵測及暴露可疑的活動。EDR 提醒您有關可能有害的活動、排定資安事端的優先順序以便快速分類，並讓您在您的潛在攻擊蒐證分析期間導覽裝置活動記錄。以便對潛在攻擊進行鑑識分析。

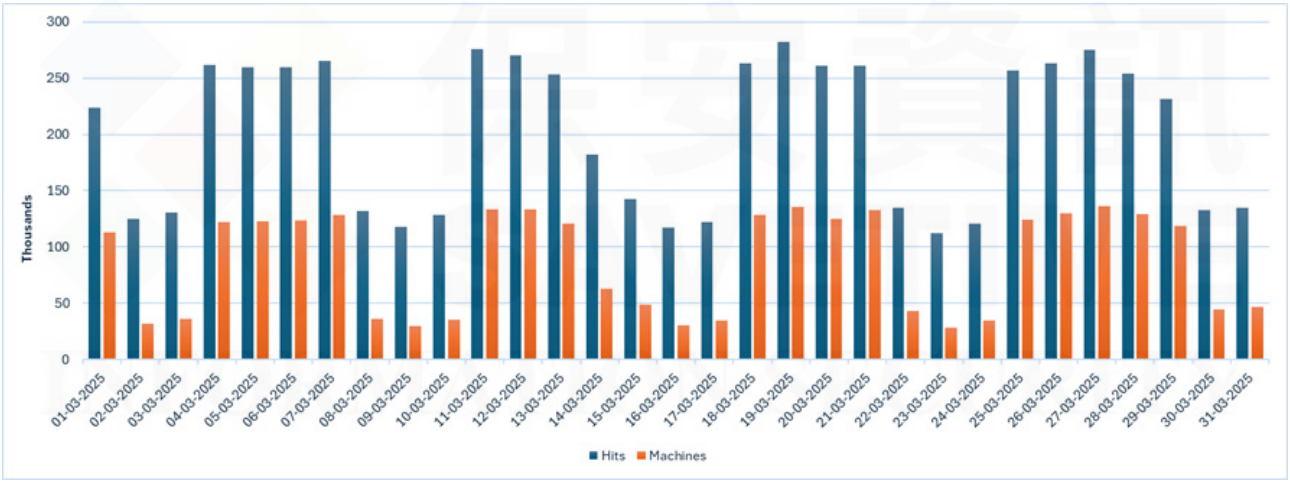
提供憑證轉存的保護

賽門鐵克 EDR 攔截憑證轉存嘗試的成效



EDR 提供憑證轉存嘗試的可視性

EDR 結合 MITRE 事件充實更新 (MITRE event enrichment updates) 提供憑證轉存嘗試的可視性



要了解更高階等級的安全防護以及端點資安持續監控與異常反應系統 (EDR)：Symantec Endpoint Detection & Response，請點擊此處。

2025/04/22

勒索軟體駭客組織：Interlock採用ClickFix社交工程誘導受害者感染惡意竊密軟體

有報導指出，勒索軟體駭客組織：Interlock 採用 ClickFix 社交工程誘導受害者感染惡意竊密軟體。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，以幾可亂真的網頁或文件外觀，誘導使用者執行惡意指令。該勒索軟體駭客組織一直在濫用已遭入侵操控的合法網站來託管惡意軟體以供下載，並展示偽造的 Cloudflare 圖靈 (CAPTCHA) 驗證機制，誘騙使用者執行 PowerShell 指令。此指令會安裝 PyInstaller 套件來執行腳本以部署 PowerShell 後門，同時將受害者被重導向合法的 Advanced IP Scanner 網站以分散注意力。除了勒索軟體之外，該駭客組織還將其工具包擴大到包括鍵盤側錄錄器和惡意竊密軟體。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Arp!g1
- ACM.Ps-CPE!g2
- ACM.Ps-Http!g2
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransomware!g7
- SONAR.Ransomware!g16
- 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：

- 'Ransom.Interlock
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Trojan.XSense.C
- 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：

- 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。

2025/04/22

Gunra勒索軟體，來勢洶洶

另一個以 Gunra 為名的勒索軟體駭客最近浮上檯面，據稱在他們的洋蔥網站上列出了幾個受害者，分別來自醫療保健、電子和飲料製造領域。最近活動中，他們部署勒索軟體在加密的檔案中冠上 .encrt 副檔名，並在多個目錄中保留檔名為 r3adm3.txt 的勒索軟體 (贖金支付) 說明文字檔。

該 (贖金支付) 說明文字檔告知受害者，他們的資料不僅被加密，還已經落入攻擊者手中。攻擊者聲稱在加密系統之前已經竊取敏感的商業資訊，並堅稱復原檔案的唯一方法是與他們聯絡以取得解密金鑰和解密工具。為了增加壓力，訊息設定五天最後期限，據稱在期限過後，如果沒有聯繫，被盜資料就會被公布在暗網上。受害者被指示下載可以隱匿行蹤的 Tor 瀏覽器、造訪指定的 .onion 網站、註冊、登入並開始溝通。

目前，駭客完整作案手法仍不清楚，不過它很可能沿用其他雙重勒索軟體的戰術、技巧和程序 (TTPs)。這些技倆通常是透過網路釣魚或竊取憑證 (通常是向黑市的初始存取掮客人購買憑證) 取得存取權限，接著使用 PowerShell、PsExec 和 Mimikatz 等工具進行橫向移動和權限提升。之後，資料會透過 Rclone 或 FTP 等服務外流，傳送前通常會先打包成壓縮檔並以密碼保護。

網路知識：Rclone 是一個開源、多執行緒、命令行界面的電腦程式，可用於管理雲端儲存。其功能包括檔案同步、文件傳輸、加密、快取和掛載。rclone 支援包括 Amazon S3 和 Google 雲端硬碟在內等共五十多種雲端儲存服務。

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
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g193
- SONAR.Ransom!gen56
- SONAR.Cryptlck!g171

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：

- Trojan.Gen.2
- Ransom.Gen

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/04/21

安卓平台出現SuperCard X惡意軟體即服務的金融詐騙行動

一起全新的 Android 惡意軟體攻擊行動，被識別為 SuperCard X 的惡意軟體即服務所發起，已被觀察到以義大利使用者為目標。此行動透過社交工程化的簡訊釣魚和電話傳送，其目的在於竊取財務資訊。

在成功入侵的情況下，受害者會被說服安裝惡意軟體，並在已感染的行動裝置附近出示一張實體卡片。惡意軟體利用 NFC 傳輸資料竊取卡片的詳細資料。網路罪犯會將這些資料傳輸到他們自己的裝置，以便在 POS 機上進行未經授權的非接觸式購物支付和 ATM 提款。

網路知識：NFC 是英文「Near-Field Communication」的縮寫，中文稱為「近場通訊」或是「近距離無線通訊」，是一種能讓裝置在短距離內進行安全且非接觸式通訊的高頻無線通訊技術，可實現快速且有效的資料交換。

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。

- AdLibrary:Generisk
- 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。

2025/04/18

PasivRobber--針對macOS平台的間諜軟體

PasivRobber 是最近在真實網路情境裡發現針對 macOS 平台的全新間諜軟體。其主要功能是從 macOS 系統中篩選出各種資料，包括來自第三方應用程式、網頁瀏覽器、電子郵件、cookie、聊天訊息 (微信和 QQ)、螢幕截圖等的資訊。PasivRobber 依賴 28 個獨立的動態函式庫，偽裝成 .gz 檔案，針對受感染系統上的不同位置進行資料收集。

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
- OSX.Trojan.Gen.2
- Trojan Horse
- WS.Malware.1

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。

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**。