保安資訊--本周(台灣時間2024/12/06)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 4,300 台受保護端點上總共阻止了 4,390 萬次攻擊。這些攻擊中有 77.8% 在感染階段前就被有效阻止：**(2024/12/02)**

- 在**8萬2,800**台端點上，阻止了**1310**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬7,600**台端點上，阻止了**800**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬6,800**台**Windows**伺服主機上，阻止了**6萬1,000**次攻擊。
- 在**4萬8,600**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬700**台端點上，阻止了**75萬5,000**次嘗試掃描在**CMS**漏洞。
- 在**4萬200**台端點上，阻止了**190**萬次嘗試利用的應用程式漏洞。
- 在**8萬6,300**台端點上，阻止了**140**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,700**台端點上，阻止了**96萬3,300**次加密貨幣挖礦攻擊。
- 在**10萬8,100**台端點上，阻止了**890**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**499**台端點上，阻止了**9萬600**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 19 萬 5,400 個受保護端點上阻止了總計 820 萬次攻擊。**(2024/12/02)**

- 使用網頁信譽情資，在 **187.1K** 個端點上阻止 **780** 萬次攻擊。
- 攔截 **19.7K** 個端點上 **255.8K** 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 **8.1K** 個端點上攔截 **172.1K** 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 **476** 個端點上攔截 **8.8K** 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。

2024/12/05

中國駭客組織鎖定中國境內的美國機構發動攻擊

總部位於中國的一家美國機構已經遭受長達數個月網路攻擊。根據已觀察到的攻擊資料，可以肯定是由一個中國的威脅組織所為。該攻擊由多個部分組成，包括但不限於以下部分：

- 就地取材工具，包括 PsExec 和 WMI
- 使用 iTunesHelper 和 GoogleUpdate 等合法應用程式側載惡意 dlls
- Impacket
- FileZilla

攻擊者建立持久性／常駐能力並透過網路橫向移動，其明顯目的是收集情報以進行外洩。

在我們的部落格中閱讀更多資訊：在中國的美國機構成為攻擊者的目標。

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.Btsad-Lnch!g1
- ACM.Ps-CPE!g2
- ACM.Ps-Http!g2
- ACM.Psxec-Lnch!g1
- ACM.Psxec-Masq!g1
- ACM.Psxsv-Net!g1

- ACM.Psxsv-Quser!g1
- ACM.Reg-Dmpsam!g1
- ACM.Wmip-Ps!g1
- ACM.Wmip-Reg!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。

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.MBT
- WS.Malware.1

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security，預設強化功能即可針對此攻擊鏈提供零時差防護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2024/12/05

日本釣魚電子郵件以抖音(TikTok)使用者為目標，提供假冒的抖音(TikTok)影片邀請

威脅份子在日本的網路釣魚電子郵件中引入新的主題，這次是偽造抖音 (TikTok) 視訊活動。在最近一次網路釣魚嘗試中，包含網路釣魚網頁的電子郵件被偽裝成假冒的抖音 (TikTok) 影音邀請，鼓勵收件者成為 VIP 會員。電子郵件本文指示使用者完成一連串的任務、發佈帶有標籤「#TikTokVIP」的影片，並邀請五位或更多朋友加入抖音 (TikTok)。若要參與並開始活動，使用者會被引誘點擊網路釣魚網頁，此網頁目的在竊取使用者的憑證。

電子郵件標頭：

- 電子郵件主旨: 💥 TikTok 動畫投稿で豪華賞品をゲット！あなたも参加しよう！?
- 翻譯後的電子郵件主旨：💥 在 TikTok 上發佈影片並獲得豐富獎品！加入我們
- 電子郵件主旨: 🎁 豪華賞品が當たる！TikTok フォロー&シェアキャンペーン🎉
- 翻譯後的電子郵件主旨: 🎁 贏取豐厚獎品！TikTok追踪 & 分享 活動🎉

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：

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。

2024/12/04

CleverSoar：全新惡意軟體安裝程式鎖定中文和越南語系的使用者

網路威脅聯盟 (Cyber Threat Alliance，CTA) 會員：Rapid7 在最近一份報告中，揭露一款新的高度迴避性惡意軟體安裝程式「CleverSoar」，其目標是針對中文和越南語系的受害者。CleverSoar 設計目的是在一個行動中部署和保護多個惡意元件，包括進階的 Winos4.0 框架和 Nidhogg rootkit。這些工具提供的功能包括按鍵記錄、資料外洩、繞過安全措施以及隱蔽地控制系統。

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：

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.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。

2024/12/04

以虛構的年終薪資報告為幌子來詐騙員工憑證

最近發現有網路釣魚行動，利用偽造的 OneDrive 文件頁面針對使用者。這是一個老奸巨猾水準的網路釣魚行動，企圖以例行的文件共享工作流程為幌子，利用惡意 HTML 檔案竊取敏感的憑證。

當使用者開啟惡意的 HTML 檔案時，會立即看到偽造的 OneDrive 逼真頁面，其目的是模仿合法的文件共享平台。該頁面採用熟悉的介面，顯示名為「Staff Salary Valuation Report for December 2024.pdf」的檔案，包含檔案大小和類型。攻擊者利用 OneDrive 的品牌和特定檔案細節，目的在讓人陷入一種虛假的信任與可信度，引誘使用者相信該頁面是真實的。

按一下「檢視文件」按鈕會觸發登入模式，要求使用者輸入電子郵件和密碼。令人吃驚的是，電子郵件欄位會預先輸入受害者的電子郵件位址，讓人覺得系統似乎辨識使用者。

一旦輸入憑證，就會立即透過 API 傳送至 Telegram 機器人。攻擊者使用隱藏的網頁收集並儲存竊取的資訊，以供日後利用。在第二次表單提交後，使用者會被重導向到看起來合法的 OneDrive 連結，以避免被懷疑。

文件的選擇絕非巧合，而是刻意設計的手法，目的在於利用工作場所的好奇心，以及對敏感組織資訊有一定的興趣。薪資報告，尤其是那些與特定時間範圍相關的報告，是高價值的文件，通常會詳細說明薪資標準、獎金和財務決定，因此對許多員工而言是無法抗拒的誘惑。

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)。

2024/12/04

全新Andromeda(*仙女座)後門程式涉入多起惡意軟體傳播活動

在真實網路情境上發現到 Andromeda(又名 Gamarue) 惡意軟體所涉入的新活動。據報道，攻擊者目標是亞洲的製造業和物流業。被傳播的 Andromeda 有效酬載具有竊取機密資訊、下載並執行任意檔案，以及提供攻擊者遠端存取遭入侵端點的功能。在最近發現到的攻擊行動中，Ipeddo 和 Pykspa 等其他惡意軟體也與 Andromeda 的 C&C 伺服器進行通訊。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspInject!gen5
- SONAR.SuspLaunch!g444
- SONAR.SuspPE!gen32
- SONAR.SuspReg!gen47

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
- Downloader
- Trojan.Gen
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malscript
- W32.Pykspa.D
- W32.Pykspa!gen1
- 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
- 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 380

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。

2024/12/04

Gafgyt惡意軟體攻擊行動鎖定欠缺安全防護，導致遠端API曝露於公開網路的Docker主機

據報導，有新的攻擊行動鎖定欠缺安全防護的 Docker Remote API 伺服器。攻擊者利用 Rust 語言寫的 Gafgyt 惡意軟體來感染配置錯誤或其他易受攻擊的伺服器。受感染機器上所存在的惡意程式可讓威脅者在後續發起各種類型的 DDoS 攻擊 (UDP、TCP 和 HTTP)。

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.Gen.MBT
- 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。

2024/12/04

Vidar惡意竊密程式持續透過遭入侵的PEC電子郵件帳號散佈

上個月已發現到數起影響義大利使用者的 Vidar 惡意竊密程式之傳播事件。攻擊者利用被入侵的 PEC 信箱進行攻擊。PEC(Posta Elettronica Certificata) 是義大利的認證電子郵件系統，廣泛用於政府機關和企業的官方通訊。Vidar 惡意竊密程式透過類似發票主旨的惡意垃圾郵件散佈。感染鏈包括使用 PowerShell 和 VBS 腳本等。攻擊者在最近散佈行動中也濫用 .top 通用頂級網域名稱 (gTLD)。Vidar 有效酬載具有廣泛的資訊竊取能力，包括竊取個人資訊、憑證、網頁瀏覽器儲存的資料、加密貨幣錢包、金融資料等。

網路上知識：PEC 代表認證電子郵件 (posta elettronica certificata)，意思是“認證郵件”。認證郵件 (PEC郵件) 與傳統郵件類似，但不同之處在於它保證寄件者身份的法律確定性、發送和接收郵件的日期和時間，以及郵件內容的真實性。

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-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。

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：

- Infostealer.Vidar
- Scr.Malcode!gen

- Scr.Malcode!gen170
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- Web.Reputation.2
- 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。

2024/12/04

網路釣魚行動利用Venom Spider惡意軟體即服務(MaaS)部署RevC2和Venom Loader等惡意軟體家族

據報導，有網路釣魚行動利用惡意軟體即服務 (MaaS) 工具 Venom Spider 部署兩個進階的惡意軟體家族：RevC2 和 Venom Loader。RevC2 的功能包括竊取憑證、遠端程式碼執行和代理網路流量。Venom Loader 是自訂的惡意軟體載入器，使用受害者的電腦名稱來對有效酬載作編碼。

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.Cscr-Cmd!g1
- ACM.Cscr-RgPst!g1
- ACM.Ps-CPE!g2
- ACM.Ps-Net!g1
- ACM.Ps-Rd32!g1
- ACM.RegRun-TWscr!g1
- ACM.Wscr-Reg!g1
- ACM.Wscr-RgPst!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：

- MSH.Downloader!gen3
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Malware.1
- WS.SecurityRisk.4

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!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: Scripting Host Processes Making Network Connections
- 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。

2024/12/04

日本Orico信用卡卡友遭受新一波網路釣魚攻擊

在日本，Orico Card 是 Orico 所發行最受歡迎信用卡之一。最近，賽門鐵克發現新一波偽裝成 Orico Card 服務的網路釣魚活動。電子郵件內容提到要檢查累積的 Orico 紅利點數，並誘使卡友點擊偽裝成 Orico 紅利點數優惠連結的釣魚網址。

電子郵件標頭：

- 電子郵件主旨(日文)：【期間限定】オリコ会員だけにオリコポイントプレゼント！
- 翻譯後的電子郵件主旨： [期間限定] 專屬於ORICO會員的 ORICO紅利積點！

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。

2024/12/04

SmokeLoader惡意軟體涉入以台灣實體單位為目標的攻擊行動

SmokeLoader 是一種模組化的惡意軟體，既靈活又適應性強。它主要作為下載器來傳送其他惡意軟體，但在最近觀察到的攻擊行動中，它會從攻擊者控制的 C&C 伺服器下載外掛程式來進行攻擊。台灣製造業、醫療保健和資訊科技業的單位已成為散佈 SmokeLoader 惡意軟體新一波攻擊行動的目標。

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.ProcHijack!g45
- SONAR.SuspInject!g31
- SONAR.SuspBeh!gen*
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Bloodhound.RTF.*
- CL.Downloader!gen12
- Exp.CVE-2017-11882!g*
- ISB.Downloader!gen80
- ISB.Houdini!gen6
- MSH.Downloader
- Scr.Heuristic!gen17
- Scr.Malscript!gen18
- Scr.Malcode!gen59
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- Trojan Horse
- WS.SecurityRisk.4
- 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

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。

2024/12/03

Money Message勒索軟體活動持續

Money Message 是 2023 年 3 月出現的勒索軟體組織，透過加密受害者的資料並威脅除非支付贖金否則洩露資料的方式進行雙重勒索攻擊。自從出現以來，他們已針對全球的組織進行攻擊，包括公司和政府單位。

主使者使用自訂的勒索軟體，以 Windows 和 Linux 系統為主要目標，也包括 VMware ESXi 伺服器。雖然他們不像其他知名的勒索軟體團體，例如：Akira、Play 或 Hunters 等那麼活躍，但他們的行動一直持續到 2024 年，受害新聞時有所聞。

最近針對 VMware ESXi 伺服器的 Money Message 勒索軟體樣本展示先進的策略能力。其中包括精確的加密技術，例如：針對重要的虛擬機器檔案 (.vmx)。此外，混淆方法 (包括 Base64 編碼) 和反鑑識手法突顯他們投入逃避偵測和提升破壞力的努力。以下是他們的主要行為：

- 從組態中獲取並列出要略過的檔案副檔名
- 搜尋 /vmfs 目錄中的虛擬機器
- 加密位於 /vmfs 中的所有 .vmx 檔案
- 嘗試使用 esxcli 停止所有虛擬機
- 在 /vmfs 目錄中建立名為 money_message.log 的檔案

留在受攻擊機器上的勒索 (贖金支付) 說明一開頭就直接聲明資料已遭洩露，包括社會安全號碼、客戶註冊詳細資料、駕照、電話號碼、電子郵件等敏感資料。攻擊者聲稱不僅取得公司資料，還取得其他組織員工簽署的文件。

攻擊者威脅要在他們的部落格上公布竊取的資料，並提供一個 .onion 連結，以便在暗網中存取這些資料。他們還建議透過協商來復原資料，並將受害者指引可透過 Tor 加密瀏覽器存取的聊天連結。為了進一步向受害者施壓，這份說明引用實際世界中因資料洩漏和相關訴訟而遭受重大損失的企業案例，包括這些案例的新聞文章連結。

整體而言，勒索 (贖金支付) 說明的設計目的在於利用機敏資料曝光、法律糾紛和聲譽受損等威脅以恐嚇和脅迫受害者支付贖金。它體現該組織使用雙重勒索策略的典範，將資料盜竊與公開披露的威脅結合起來，以最大化他們的籌碼。

由近期取得 Money Message 勒索軟體二進位檔所剖析後的 TTPs(戰術、技巧與程序) 包括：

- 命令和腳本直釋器：Unix Shell [T1059.004]
- 命令和腳本直釋器 [T1059]
- 命令和腳本直釋器：Python [T1059.006]
- 損害防禦：停用或修改工具 [T1562.001]
- 檔案與目錄發現 [T1083]

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.MoneyMess

2024/12/03

防護亮點：賽門鐵克調適型防護(Adaptive Security Protection) 有效對抗 Ymir 勒索軟體

Ymir 的出現

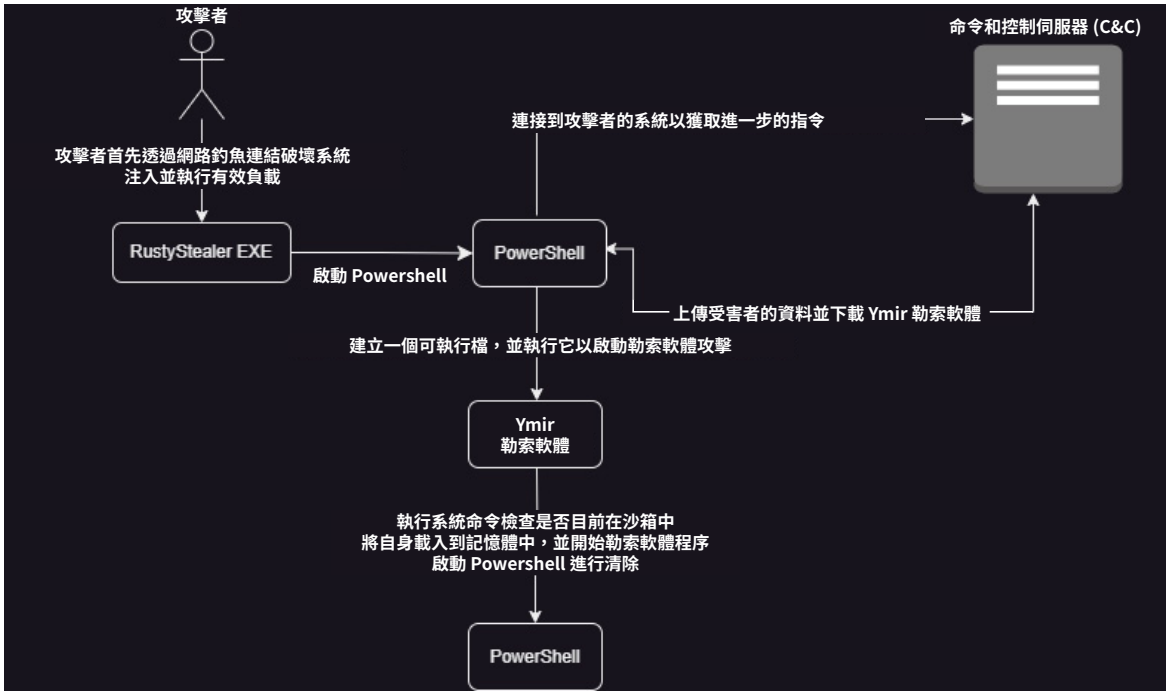
近期出現全新勒索軟體：Ymir，目標是哥倫比亞的一個組織。它利用先進的記憶體管理功能來執行惡意程式碼，並將惡意竊密程式 RustyStealer 整合到其攻擊鏈中。透過採用創新策略，Ymir 繞過許多針對現有勒索軟體家族所設計的安全防護措施。然而，賽門鐵克的調適型防護 (Adaptive Security Protection) 已經證明有能力降低此類新興威脅的風險。調適型防護 (Adaptive Security Protection) 可中斷攻擊鏈，即使是針對前所未見的威脅。

調適型防護(Adaptive Security Protection)：奠定端點防護日後長期發展的策略優勢

勒索軟體攻擊者通常會濫用，就像一般使用者或 IT 管理員操作的軟體或管理工具，這在資安範疇稱為就地取材 (LOTL：Living Off the Land) 攻擊。由於這些軟體或管理工具在組織內有其正當的用途，因此完全停用並不可行。雖然不同的攻擊者會個別修改特定步驟以逃避偵測，但他們對 LOTL 的依賴程度，相當一致。調適型防護 (Adaptive Security Protection) 以有益的方式解決這些挑戰，更可讓組織在不中斷其正當操作的情況下阻止 LOTL 攻擊。

Ymir 攻擊鏈：關鍵事件與防禦

下圖拆解成一個個步驟來說明 Ymir 勒索軟體攻擊鏈，凸顯其與 RustyStealer 惡意軟體和 PowerShell 的整合，以執行與其命令與控制 (C&C) 伺服器的通訊。



調適型防護 (Adaptive Security Protection) 在攻擊鏈的不同階段皆能有效力抗 Ymir 攻擊：

行　　為	調適型防護	曾出現在過往的勒索軟體攻擊？
執行 RustyStealer (不受信任的程序)	是	否
不受信任的程序執行 Powershell 指令碼，並與控制伺服器建立連線	是	是
Powershell 腳本上傳檔案	是	是
Powershell 執行 Base64 指令	是	是
InfoStealer 會建立 PE 檔案 (勒索軟體範例)	是	是
InfoStealer 會啟動 PE 檔案 (勒索軟體範例)	是	是
執行勒索軟體樣本	是	是
勒索軟體樣本啟動 Powershell	是	是

數字會說話：調適型防護 (Adaptive Security Protection) 有效力抗 Ymir 勒索軟體攻擊鏈

- 追蹤的行為： 橫跨 70 種應用程式的 493 種行為
- 受保護的端點： 超過 290 萬個
- 拒絕模式使用量： 客戶每次部署平均封鎖 342 個行為

調適型防護 (Adaptive Security Protection) 可確保對 Ymir 及類似演進中勒索軟體威脅進行強大的防禦，同時維持組織的作業效率。想要立即啟用 Adaptive Protection？查看以下連結了解詳情。

欲深入瞭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。
欲瞭解賽門鐵克端點安全完整版(SESC)的調適型防護(Adaptive Security Protection)，請點擊此處。

2024/12/03
擁有十八般武藝的Akira勒索軟體全新變種

Howling Scorpius 勒索軟體集團是 Akira 勒索軟體即服務 (RaaS) 幕後藏鏡人。Howling Scorpius 的目標是澳洲、歐洲和北美各行各業 (例如：顧問諮詢、教育、政府、製造、科技、電信和製藥) 的中小型企業。該組織採用雙重勒索戰略，先從網路中滲出關鍵資料，再執行加密程序。該組織採用多種方法取得對組織的初始存取權--例如：瞄準未經多因子認證機制 (MFA) 的脆弱 VPN 服務、採用不安全的遠端桌面 (RDP) 服務對外服務，以及發動魚叉式網路釣魚攻擊。

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：

自適應防護技術(包含於SESC)：

- ACM.Wmip-Ps!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.RansomAkira!g2
- SONAR.RansomPlay!gen1

- SONAR.SuspLaunch!g289
- 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：

- CL.Suspexec!gen158
- Linux.RansomAkira!g1
- Ransom.Akira!g1
- Ransom.Akira!g2
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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

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。

2024/12/03

GodLoader濫用Godot開放原始碼遊戲引擎來散佈惡意軟體

根據 Checkpoint 研究人員最近報告，GodLoader 惡意程式最新後繼變種一直在利用一種新技術進行有效酬載傳播。攻擊者濫用 Godot Engine(是一款熱門的多功能、跨平台的 2D 與 3D 開放原始碼遊戲引擎)。來執行特製的 GDScript (.gd) 檔案，進而導致惡意的二進位有效酬載的下載。下載程式以 .pck 檔案的形式出現，而 .pck 檔案是 Godot Engine 用來捆綁各種資源或資產套件的預設檔案格式。利用 Godot 遊戲引擎，攻擊者可以將惡意軟體二進位檔散佈到各種架構，包括 Windows、Linux 或 macOS。最近觀察到的 GodLoader 散佈行動會傳播 XMRig 挖礦程式或 Redline 惡意竊密程式的有效酬載。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspDriver!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：

- Downloader
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Coinminer!g3
- 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

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。

2024/12/02

惡意Python模組：Aiocpa，透過PyPI散播

威脅研究人員最近觀察並發現一個名為“aiocpa”的惡意 Python 模組，該模組在 PyPI 上發佈，其目的是入侵加密貨幣錢包。與典型攻擊不同，惡意行為者建立自己的加密用戶端以吸引用戶，然後透過惡意更新對其進行攻擊。

維基百科知識：PyPI(英語：Python Package Index，簡稱 PyPI) 是 Python 正式第三方 (official third-party) 軟體套件的軟體儲存庫，它類似於 CPAN(Perl的儲存庫)。一些軟體套件管理器，例如：pip，就是預設從 PyPI 下載軟體套件。使用者通過 PyPI 可以下載超過 235,000 個 Python 軟體套件。

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
- WS.Malware.1

2024/12/02

針對墨西哥多個行業的假冒液化石油氣經銷商的活動

2024 年 11 月下半月，有人觀察到一名威脅者假冒墨西哥一家知名的液化石油氣 (L.P. Gas) 經銷商，該經銷商提供一系列服務，包括為住宅和商業客戶銷售和加注瓦斯鋼瓶和固定式儲罐。此活動針對當地多個跨領域的行業及國際組織 (在該國設有辦事處)，包括石化、金融服務、能源、製造業、旅館業及零售業。

這封惡意電子郵件 (主旨：Estado de cuenta) 是利用一般的「帳戶對帳單」社交工程伎倆，寄件者的訊息簡潔明確，並將重點放在其目的上。接著是隱私權政策宣告的字句，提到墨西哥聯邦個人資料保護法第 3 條和第 14 條，試圖讓電子郵件看起來更值得信任。

如果使用者被成功誘騙解壓所附的 ARJ 壓縮檔 (Estado de cuenta PDF.arj) 並執行其中所含的二進位檔 (Estado de cuenta.exe)，他們最後就會被惡意軟體入侵，而惡意軟體會同時扮演後門及惡意竊密程式的角色。惡意軟體使用大量混淆、加密字串，並執行 .NET 組合程式碼，儘管其初始二進位檔並非 .NET 可攜式執行檔 (PE)。隱藏在記憶體中的某些模組是專為以下目的設計：

- 與遠端伺服器建立連線並監聽指令
- 直接在記憶體中下載和執行附加的 .NET 模組

它還具有列出執行中的程序、終止指定的程序、下載外部檔案、將其作為程序執行，以及竊取敏感資訊的能力。

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：

基於行為偵測技術(SONAR)的防護：

- 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。

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：

- Trojan.Gen.MBT

2024/12/01

花兩百美元就能取得「Rockstar 2FA」網路釣魚工具包(網路釣魚即服務)

研究人員最近揭露「Rockstar 2FA」這是一種網路釣魚工具包，它可以透過中間人 (AiTM) 攻擊來竊取憑證並繞過多因素認證 (MFA)。此網路釣魚即服務 (PaaS) 的售價從 200 美元起跳，並自 2024 年 8 月起開始活躍。它以 Microsoft 365 帳戶為目標，使用汽車為主題的假冒登入頁面，根據報告，已識別超過 5,000 個網域。在最近的攻擊行動中，攻擊者利用已洩露的帳戶和合法的電子郵件平台來傳送網路釣魚連結，將受害者引導至幾可亂真但偽造的假冒入口網站。

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：

- Attack: WordPress Really Simple Security CVE-2024-10924

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**。