保安資訊--本周(台灣時間2024/11/29)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 39 萬 6,300 台受保護端點上總共阻止了 4,630 萬次攻擊。這些攻擊中有 78.4% 在感染階段前就被有效阻止：**(2024/11/25)**

- 在**9萬100**台端點上，阻止了**1,400**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬5,900**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**2萬7,800**台**Windows**伺服主機上，阻止了**7**萬次攻擊。
- 在**5萬3,200**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬8,200**台端點上，阻止了**77萬7,300**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,000**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**9萬3,000**台端點上，阻止了**170**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,900**台端點上，阻止了**95萬6,800**次加密貨幣挖礦攻擊。
- 在**10萬8,600**台端點上，阻止了**910**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**492**台端點上，阻止了**8萬3,000**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 19 萬 8,400 個受保護端點上阻止了總計 820 萬次攻擊。**(2024/11/25)**

- 使用網頁信譽情資，在 **189.7K** 個端點上阻止 **770** 萬次攻擊。
- 攔截 **20.9K** 個端點上 **282.3K** 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 **8.6K** 個端點上攔截 **157K** 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 **437** 個端點上攔截 **9.3K** 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。

2024/11/28
CVE-2024-10924--存在WordPress外掛Really Simple的身分鑑別繞過漏洞

CVE-2024-10924 是一個最近被揭露嚴重等級 (CVSS風險評分：9.8) 的身分鑑別繞過漏洞，會影響 WordPress 外掛 Really Simple。此漏洞是由於該外掛的雙重認證 REST API 不當處理使用者認證所造成。若該漏洞被開採濫用，未經認證的攻擊者可完全管理受影響系統的存取權限。估計約有 400 萬個 WordPress 網站使用受影響的 Really Simple Security 外掛程式。此漏洞影響 9.0.0 至 9.1.1.1 的外掛版本，而修補程式已於 9.1.2 更新中發佈。

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：

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

2024/11/28
Wish Stealer惡意竊密程式

Wish Stealer 是最近在真實網路情境裡發現全新惡意竊密程式。這個基於 Node.js 惡意軟體以擷取敏感的使用者資訊為目標，包括憑證、儲存在 Chromium 和 Firefox 瀏覽器中的資料、cookie、加密貨幣錢包、剪貼簿、「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼加密)、雙重認證 (2FA) 的一次性代碼或來自各種第三方應用程式 (例如：VPN 或社交媒體應用程式) 的資料。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Cscr!g1
- ACM.Ps-Net!g1
- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g399

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer.Wish!g1

2024/11/28

CVE-2024-48217--存在SiSMART中不安全的物件參照(IDOR)漏洞

CVE-2024-48217 是最近被揭露不安全的物件參照 (IDOR) 漏洞，會影響 7.4.0 或以上版本的 SiSMART dashboard。若成功開採濫用該漏洞，攻擊者可在受影響的系統上提升權限，並存取、修改或刪除其他使用者的資料，包括敏感或其他機密資訊。

網路上的知識：IDOR 全名為 Insecure Direct Object Reference，中文是不安全的物件參照，是一種存取控制類型的漏洞，該漏洞的原理是針對參數存取權限設計不完善，導致攻擊者可存取開發者料想之外的物件。

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：

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 的 IPS 政策可以控制那些程式可以在自訂 SiSMART 沙箱中執行。
- DCS 也可以控制那些資源可以在系統上寫入或讀取。它還能防止使用者資料被竊。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/11/28

CVE-2021-41277--免費開源的BI(Business Intelligence)工具：Metabase GeoJSON API本機檔案包含(LFI)漏洞在真實網路情境裡被利用

CVE-2021-41277 是一個已存在三年之久的 Metabase 陳年漏洞，最近才又被報導在真實網路情境裡再次被利用。此漏洞可讓未認證的攻擊者以 root 權限下載任意檔案，並透過特製的 HTTP GET 請求存取環境變數。隨著在真實網路情境裡已遭大肆開採濫用攻擊的報告，此漏洞也在本月初被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

網路上的知識：本機檔案包含 (LFI) 漏洞成因在於後端程式 PHP 語言使用 include 引入其他 php 檔案時，沒有去驗證輸入的值或是惡意攻擊者繞過驗證，導致敏感資料外洩 (etc/passwd)，而敏感資料外洩的資料是在伺服器 local 端，所以這個漏洞叫做 local file inclusion。

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: Metabase LFI CVE-2021-41277

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 強化功能，針對 Metabase 應用程式可以用多種方式降低攻擊面和暴露程度，以達到下列目的：

- 鎖定 metabase 網路暴露，讓此漏洞無法透過公共網際網路被利用。
- 防止存取作業系統關鍵檔案或環境變數，使敏感的系統資訊不會外洩。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/11/27

觀察到SpyLoan手機APP，在威脅生態圈越來越活躍

據報導，SpyLoan 手機 APP 在行動威脅領域的活動越來越多。SpyLoan 手機 APP 通常被歸類為 PUAs(潛在不需要的應用程式)，會利用各種技術危及受害者的機密資料，並可能導致財務損失。這類應用程式通常使用誘人的財務誘惑，向受害者提供貸款或承諾快速取得資金。攻擊者被滲出的資訊也可能導致受害者受到騷擾或金錢勒索。McAfee 研究人員報告指出，最近 SpyLoan 應用程式在南美洲、東南亞和非洲各國的活動增加。

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
- AppRisk:Generisk

2024/11/27

Matrix駭客集團最近針對脆弱的物聯網裝置(IoT)和雲端服務供應商(CSP)發動網路攻擊

據報導，在真實網路情境裡發現的全新網路攻擊活動，被認為出自Matrix 駭客集團之手。攻擊者一直熱衷於部署 Mirai 和 Pybot 這兩種惡意軟體來發動分散式阻斷服務攻擊 (DDoS：Distributed Denial-of-service Attack)，鎖定目標是存在已知漏洞或脆弱／預設組態的路由器、數位影像錄影主機 (DVR)、網路攝影機或其他物聯網裝置 (IoT)。最近攻擊活動也顯示攻擊者更加專注針對雲端服務供應商 (簡稱 CSP：Cloud Service Providers) 的伺服器和基礎架構。

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：

- Hacktool
- Linux.Lightaidra!g1
- Linux.Mirai
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

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: Zyxel Firewall Unauthenticated Command Injection CVE-2022-30525
- Web Attack: DVR Authentication Bypass CVE-2018-9995
- Web Attack: Gpon Router Cmd Injection CVE-2018-10561
- Web Attack: Gpon Router Cmd Injection CVE-2018-10562
- Web Attack: Huawei Router RCE CVE-2017-17215
- Web Attack: Realtek SDK RCE CVE-2014-8361

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。

2024/11/27

Citrix Virtual Apps and Desktops虛擬化解決方案的元件存在：CVE-2024-8068、CVE-2024-8069兩個遠端程式碼執行(RCE)漏洞

Citrix Virtual Apps and Desktops 是虛擬化解決方案，可讓 IT 管理員控制虛擬機器、應用程式、授權和安全性，同時可從任何裝置進行隨處存取。研究人員在應用程式的 Session Recording Manager 元件中發現兩個遠端程式碼執行 (RCE)漏洞--(CVE-2024-8068、CVE-2024-8069)。Session Recording 的工作原理，即是對會話進行記錄、編錄和存檔，以便進行檢索和播放。此元件可讓系統管理員擷取使用者活動，以進行稽核、合規性及故障排除。這個問題是由於 Session Recording Manager 將資料轉換成方便儲存與傳輸的格式時，在資料反序列化的方式上產生弱點。賽門鐵克的端點防護系列解決方案 (SEP／SES／EDR) 上的網路層安全技術--入侵防護系統 (IPS) 能有效阻止利用這些漏洞的嘗試，防止系統受到進一步感染或損害。

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: Malicious Payload Upload 25

2024/11/26
防護亮點：賽門鐵克進階機器學習(AML)攔截零時差攻擊

賽門鐵克如何利用進階機器學習(AML)技術防禦零時差威脅

機器學習 (Machine Learning)，通常簡稱為 ML，是一種無須特徵檔的技術，可在執行前階段攔截全新的惡意軟體。在博通賽門鐵克 (Broadcom-Symantec) 裡，ML 用於不同層級，以保護我們的客戶免受網路威脅。這些層級的設計可主動或被動「監控」我們產品所看到的可疑檔案、作業系統事件、登錄檔、網頁位址或網路活動的每個位置--包括端點、閘道和我們的後端分析平台。賽門鐵克能夠透過一套完整的威脅掃描引擎，在新內容出現時立即進行動態分析，並將資料擷取至賽門鐵克全球智慧網路 (GIN)。賽門鐵克使用來自數百萬個端點的安全遙測資料、來自第三方安全供應商的威脅相關資料饋送，以及豐富的乾淨檔案集，來訓練和評估各種 ML 模型。這些模型部署在許多產品上，以偵測威脅，包括作為我們代理程式一部分的客戶端點，以及我們的後端分析系統。

零時差保護非常重要

除了上述的分析平台之外，我們還運用雲端沙盒分析引擎 (Cloud Sandbox Analysis Engine)(非常適合的名稱「Cynic」)，執行多種 ML 模型和叢集演算法，根據威脅類型、潛在風險、動態和靜態元資料以及行為，對檔案進行分類和叢集。賽門鐵克利用自動化系統和人工的惡意軟體分析師盡快分析客戶提交的資料，並將情報擷取至 ML 訓練模型，以改善分類效能。我們的多模型進階機器學習技術可在 32 位元和 64 位元版本的各種檔案類型上執行，以提供可行的分析。當發現防護力有落差時，這些落差會由後端 ML 模型進行分析，並透過 Reputation lookups (信譽查詢) 迅速攔截。賽門鐵克進階機械學習的主要目標是防護全新的未知惡意軟體，也就是業界常說的零時差攻擊。這正是 ML 的優勢所在。

在上個季度，賽門鐵克的進階機器學習防護技術在賽門鐵克端點和閘道產品上攔截超過 1,800 萬個威脅。其中約有 260 萬個攔截是針對零時差攻擊，也就是我們的安全產品或防護技術從未見過的攻擊，這就是所謂「主動式」防護。與「被動式」防護不同，「被動式」防護是指針對攻擊增加新防護措施或更新現有的防護措施。主動式防護是對抗網路威脅的靈丹妙藥，也是各地潛在網路罪犯的剋星。

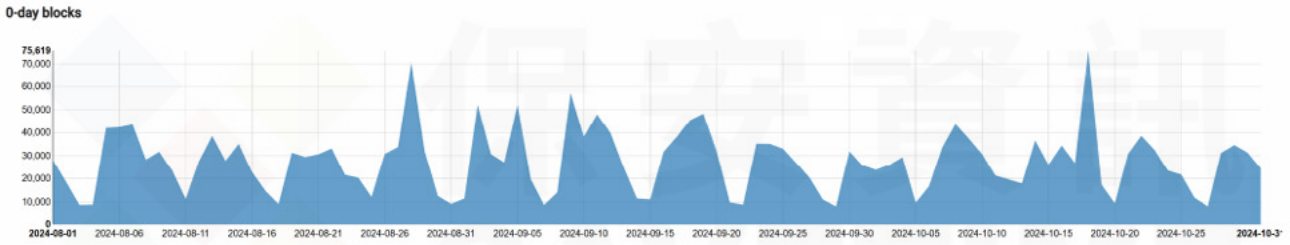
賽門鐵克進階機器學習防護技術在過去一個季度所提供的保護數據：

- 賽門鐵克 Advanced ML 在閘道產品上封鎖 1,240 萬個威脅
- 在端點上封鎖 580 萬個威脅
- 攔截 260 萬個零時差威脅，包括
  - 1 萬 6 千個勒索軟體 (HiddenTear、Gandcrab、Ryuk、Wannacry、Zombie、CryptoJoker、PureCrypter、Expiro 等)

- 36 萬 5 千個 木馬程式 (Asprox, Cidox, BumbleBee, Cryect, CoinMiner, JokLoader, Nancrat, ToralDrop, WhisperGate, GenKryptik, AsyncRAT, Remcos, AgentTesla, Lokibot, LummaStealer, ZBot 等)
- 11 萬個 Win32 (Babonock, Beapy, Cridex, Extrat, Qakbot, Fujacks, Wabot, Zorex, etc.)
- 15 萬 5 千個 後門程式 (Wecoym、Rifelku、Matsnu、Ghostnet、Cobalt、Breut 等)

- 在端點封鎖 170 萬個瀏覽器型威脅--41% 來自 Chromium、28% 來自 MS Edge、8% 來自 Firefox
- 攔截 150 萬個嘗試從 USB 磁碟機等外部來源進入系統的威脅
- 在端點產品上封鎖 140 萬個透過命令列下載並執行惡意檔案的威脅
- 封鎖 13 萬 5 千 個使用點對點 (P2P) 網路程式下載的威脅，例如：Anydesk (RDP)、Utorrent 和 Bittorrent
- 封鎖 3 萬 7 千個 使用 SMB 進行網路檔案分享的攻擊
- 封鎖 9 千 300 個使用腳本主機 (WSH) (Powershell/cscript/wcript) 下載的威脅

在本季度內選擇端點和閘道的零時差保護措施



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。
欲深入瞭解賽門鐵克雲端沙盒分析引擎 (Cynic)，請點擊此處。
欲深入瞭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。

2024/11/25

小心 網路釣魚～觸發Ursnif銀行木馬程式

研究人員最近發現一個網路釣魚行動，目標是美國的商業專業人員。該攻擊涉及一個含有偽造的 PDF、 LNK 檔案之 ZIP 壓縮檔。開啟檔案後，會執行一個惡意 HTA 檔並啟動 Ursnif 的銀行木馬程式。Ursnif 會連接到遠端伺服器，下載其他惡意軟體並竊取敏感資訊。

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：

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!gen171

- Trojan.Gen.NPE
- 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。

2024/11/25

Hexon惡意竊密程式～以威脅者自己名字命名的惡意軟體

今年 8 月，有人在 Telegram 頻道觀察到一個名為「Hexon Stealer」用戶在推廣一款以自己名字命名的惡意軟體，該惡意軟體設計目的是竊取「Discord Token」(建立帳戶時產生的 Discord 使用者名稱和密碼的加密)、雙重認證 (2FA) 的一次性代碼、密碼和加密貨幣的詳細資料。該惡意軟體可以完全操控遭入侵的遠端系統，讓攻擊者可以控制裝置，並可能進行勒索談判。支付贖金是透過 Coinbase 加密貨幣交易所進行，讓交易無法追蹤。

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
- WS.Malware.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。

2024/11/25

近期加密貨幣飆漲可能引發更多網路相關攻擊

最近加密貨幣市場的飆升--無論是實際的加密貨幣價值、ETF 或加密貨幣交換平台--都因美國在最近幾週支持加密貨幣的立場而得益。先前加密貨幣市場的飆升，已帶動網路威脅的增加；因此，人們對數位資產的興趣提高，很可能會吸引網路罪犯，導致加密貨幣相關威脅增加，包括網路釣魚攻擊、加密劫持、非法挖礦，以及假冒的投資平台和拋售詐騙等行為，這些詐騙持續剝削投資人，往往造成重大財務損失。

這些威脅同時以桌上型電腦和行動平台為目標，突顯出需要對各種裝置提高警覺。例如：最近一場攻擊行動假冒 Coinbase 加密貨幣交易所，向美國用戶發送包含的惡意網址的簡訊內容，將受害者重導向至一個詐騙網站，目的在竊取他們 12 個字元的恢復助記詞。這類行動提醒使用者要保持謹慎，避免分享敏感的錢包資訊。

網路上知識：恢復短語 (Recovery Phrase 或「助記詞」) 是首次設置加密資產錢包(例如：MetaMask) 時，系統自動產生的多組詞語。 技術上，它是錢包私鑰 (private key) 的一種表現方式

，方便用戶記錄和記憶。用戶一旦忘記錢包登入密碼，也可用它作「後備密碼」復原帳戶。

以 BIP-39 標準為基礎的 12 個字元恢復助記詞是加密貨幣錢包的主要安全功能。它由 2048 個字元清單中挑選出的 12 個字元組成，目的在方便記憶和書寫。這個助記詞代表錢包的私人密碼鑰匙，方便備份和還原。如果助記詞被盜，竊賊可能就能進入錢包並轉移資金。

BIP39 (Bitcoin Improvement Proposal 39) 是比特幣改進提案第 39 號，由 Marek Palatinus 和 Pavol Rusnak 等人於 2013 年提出，並成為行業標準之一。

觀察到的惡意簡訊：

- **Coinbase wallet Alert:** Your account requires immediate verification to avoid a permanent block. Please verify at hxxps[:]//wv3[.]io/jfPDDz7z within 4 hours to ensure continuous access.
  (**Coinbase wallet Alert:** 您的帳戶需要立即驗證以避免永久封鎖。請在 4 小時內於 hxxps[:]//wv3[.]io/jfPDDz7z 進行驗證，以確保持續存取。)

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。WebPulse 已知道此次活動中使用假冒的 IRS 域名。

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。

2024/11/25

假冒加拿大終端物流服務商：Dragonfly-Intelcom的詐騙帳密／憑證釣魚行動

賽門鐵克新發現一起假冒加拿大終端物流服務商：Dragonfly-Intelcom 的詐騙帳密／憑證釣魚行動。Dragonfly-Intelcom 是一家位於魁北克省蒙特利爾市的全球包裹遞送公司，在這一波攻擊中被利用。釣魚電子郵件偽裝成包裹遞送通知，建議收件人重新安排遞送時間或檢查包裹細節。這些電子郵件包含一則簡短的訊息，其中的惡意連結會導向到專門蒐集憑證的惡意網站。

電子郵件標題：

- 電子郵件主旨：Update: Delivery Notification for Item
- 電子郵件寄件人：Dragonfly Notification <偽造的電子郵件地址>

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。

2024/11/25

Gelsemium進階持續威脅(APT)駭客集團部署多種Linux版本的後門程式

據報導，與中國有聯繫的 Gelsemium 進階持續威脅 (APT) 駭客集團已經發佈多個 Linux 後門。第一個後門稱為 WolfsBane，是 Gelsemium 的 Windows 上 Gelsevirine 後門對應在 Linux 下之版本。它的特色是開放源碼 UserLand rootkit 的隱藏程式。另一個被稱為 FireWood 的後門則與該駭客集團的 Project Wood 惡意軟體有關，其 Windows 版本已用於先前的行動中。這些工具的設計目的是利用提供網際網路服務的 Linux 系統漏洞，針對系統資訊、憑證和特定檔案進行攻擊。

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.Ps-Wscr!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：

- Hacktool
- Hacktool.Jsprat
- Linux.Mirai
- Trojan Horse
- Trojan.Gen.NPE
- 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。

2024/11/25

不斷改版的XorBot殭屍網路

XorBot (也稱為 Masjesu) 是一個相對較新且不斷演進的殭屍網路家族，早在 2023 年 11 月首次被發現，之後一直是一個重大的威脅，已知以物聯網 (IoT) 裝置為目標。它具有先進的反追蹤功能，且更新頻繁，目前版本為 1.04。其經營者也提供分散式阻斷服務攻擊 (DDoS：Distributed Denial-of-service Attack) 的租用服務。

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：

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.Gen.NPE
- 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。

2024/11/24

Termite勒索軟體

Termite 是一家勒索軟體 (資料竊取、勒索和加密) 駭客組織，最近在法國、加拿大、德國、阿曼和美國有幾個組織成為受害者，目標行業包括政府機構、教育、殘障支援服務、石油和天然氣、水處理和汽車製造。該駭客組織標誌以藍色造型的白蟻為特色，背景圖案是密密麻麻的電路圖。

他們似乎使用惡名昭章的 Babuk 勒索軟體修改版本。當該勒索軟體在機器上執行時，它會加密目標檔案，並冠上 .termite 副檔名。它還會注入內容簡短的勒索 (贖金支付) 說明文字檔 (How To Restore Your Files.txt)。攻擊者會提供他們的 Onion 加密網站，以及支援認證碼和電子郵件地址。當受害者連接到他們的網站時，會看到一個設計用來與攻擊者直接溝通的表單。表單包括輸入公司名稱、情況描述、受害者全名、電子郵件地址和「支援認證碼」的欄位。

駭客的完整作案手法仍不明確，但駭客很可能使用大多數勒索軟體駭客所使用的戰術、技巧和程序 (TTPs)，例如：透過網路釣魚、漏洞或購買的憑證取得初始存取權，並提升權限以控制網路。他們會在加密檔案的同時滲出敏感資料，要脅若不支付贖金，就會在公開網站上洩露竊取的資訊。他們會停用備份和防護功能，確保受害者無法輕易復原資料。交涉方式是透過贖金通知書、加密頻道和 TOR 網站來處理，並要求支付加密貨幣。

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：

- Ransom.Babuk

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/11/22

Ledge加密貨幣冷錢包使用者成為新一波網路釣魚覬覦的目標

Ledge 加密貨幣冷錢包，提供使用者買賣、儲存、交換及管理加密貨幣等服務。最近，賽門鐵克觀察到假冒 Ledge 加密貨幣冷錢包服務的網路釣魚活動，並誘使使用者開啟偽造的通知郵件。電子郵件本文內容提到使用者需要更新並重新啟用服務，才能繼續使用 BTC、ETH、XRP、ERC20、BEP20、TRON、TRC20 等的網服務路。用戶會收到偽裝成「Go to update」連結的釣魚網址--企圖引誘用戶打開並點擊釣魚網址，以竊取憑證。

電子郵件標題：

- 電子郵件主旨：Update(*更新提示)
- 電子郵件寄件者："Ledger" <偽造的電子郵件地址>

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。

2024/11/22

ViperSoftX惡意竊密程式已進化到有能力劫持cmdlets以隱藏其活動和逃避偵測

ViperSoftX 是一款可追溯至 2020 年的惡意竊密程式，最近有報告指出該程式利用新的技倆來逃避偵測。傳統上，ViperSoftX 著重於竊取加密貨幣、主機指紋圖譜 (Fingerprinting)、剪貼簿劫持／置換，以及允許在受感染系統上執行其他惡意有效酬載。現在，它增加動態產生和更改 C&C 網域的能力，以及劫持 Resolve-DnsName PowerShell cmdlet 以隱藏其活動和逃避偵測。

網路上的知識：Cmdlet 是在 PowerShell 環境中使用的輕量型命令。PowerShell 執行時間會在命令列所提供的自動化腳本內容中叫用這些 Cmdlet。 PowerShell 執行時間也會透過 PowerShell Api 以程式設計方式叫用它們。

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!g

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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.2
- Trojan.Gen.9
- Trojan.Gen.MBT
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!400
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.C
- Heur.AdvML.D

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：

- URL reputation: Browser navigation to known bad URL

2024/11/22

NodeStealer惡意竊密程式的後繼新變種，正鎖定「臉書廣告管理員／Facebook Ads Manager」帳戶

據報導，由 Python 撰寫而成且以「臉書廣告管理員／Facebook Ads Manager」帳戶為目標的 NodeStealer 惡意竊密程式已有後繼新變種。Facebook Ads Manager 是一款用於管理多個社交媒體平台（包括 Facebook 和 Instagram）廣告活動的工具。過去，NodeStealer 曾以 Facebook Business 帳戶為目標，收集登入憑證、cookie 和儲存憑證。較新的變種還能從受害者的 Facebook Ads Manager 帳戶中擷取更多資訊，並利用這些資訊建立惡意的 Facebook 廣告。

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-FlPst!g1
- ACM.Ps-Http!g2

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.Dropper!gen4
- Trojan Horse
- Trojan.Gen.NPE
- 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
- Audit: Untrusted Telegram API Connection

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**。