保安資訊--本周(台灣時間2022/08/05)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 95 萬 4,600 個受保護端點上總共阻止了1.629億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/07/31)**

- 在**18萬8,600**台端點上，阻止了**7,430萬**次嘗試掃描**Web**服務器的漏洞。
- 在**36萬6,000**台端點上，阻止了**3,690萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬700**台**Windows**伺服主機上，阻止了**1,990萬**次攻擊。
- 在**13萬5,900**端點上，阻止了**770萬**次嘗試掃描伺服器漏洞。
- 在**6萬4,900**台端點上，阻止了**320萬**次嘗試掃描在**CMS**漏洞。
- 在**10萬1,900**台端點上，阻止了**310萬**次嘗試利用的應用程式漏洞。
- 在**30萬100**台端點上，阻止了**780萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5萬2,000**台端點上，阻止了**400萬**次加密貨幣挖礦攻擊。
- 在**46萬1,000**台端點上，阻止了**590萬**次向惡意軟體**C&C**連線的嘗試。
- 在**5,600**台端點上，阻止了**17萬3,500**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。

2022/08/04

Mars Stealer 竊密惡意軟體透過一個偽造 Atomic Wallet 網站傳播

Mars Stealer 是一種針對用戶憑證、加密貨幣錢包和雙因子 (2FA) 外掛程式等的資訊竊取惡意軟體變種。最近看到該惡意軟體透過一個偽造 Atomic Wallet 網站傳播。該網站向任何想要下載Windows 版加密貨幣錢包的人，提供一個包含惡意批次檔的 ZIP 檔案。批次檔一旦執行，透過一系列 PowerShell 命令，將導致從攻擊者的 Discord 伺服器下載 Mars Stealer 有效籌載來進行後續攻擊。

節錄網路：Atomic Wallet 是基於裝置智慧機制和跨鏈技術的去中心化錢包。

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：

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：

- System Infected: Bad Reputation Process Request 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已於第一時間收錄於不安全分類列表中。

2022/08/04

在真實網路環境發現 Woody RAT 遠端存取木馬惡意軟體到處亂竄

Woody RAT 是一個經客製化的遠端存取木馬，在各種活動中活躍至少一年時間。該惡意軟體主要是透過利用 MSDT Follina（CVE-2022-30190）漏洞的惡意檔案和 MS Office 文件檔進行傳播。Woody RAT 的功能包括收集有關受感染系統的各種資訊、遠端命令執行、下載額外的任意檔案或有效籌載以及執行從 C&C 伺服器收到的命令。

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(Snoar)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2

- Trojan.Gen.MBT
- W97M.Downloader
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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: MSDT Remote Code Execution CVE-2022-30190
- 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已於第一時間收錄於不安全分類列表中。

2022/08/03

Linux 威脅環境中的 RapperBot 殭屍電腦／機器人

自從 Mirai 首次出現在威脅領域以來，一直不乏具有分散式拒絕服務 (DDoS) 能力的 Linux 機器人，其目標是物聯網 (IoT) 設備。這些機器人中不時就會出現另一個 (基於 Mirai 程式碼) 展現嚴重程度的後起之秀，例如：RapperBot。根據報告，這種威脅位於被入侵的物聯網上，掃描 SSH 伺服器並試圖對其進行暴力攻擊。如果成功，它將向其命令和控制伺服器回報憑證，然後在 SSH 伺服器上部署自己。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai

2022/08/03

他山之石可以攻錯～日本出現重複性的電子道路收費系統 (ETC) 網路釣魚活動

日本民眾繼續成為網路釣魚行動的目標，在這些行動中，威脅者冒充 ETC (電子道路收費系統)--透過高速公路收費站的天線和車載設備之間的無線通訊來支付通行費。在過去的幾週裡，賽門鐵克在電子郵件和行動威脅防護領域都觀察到這些行動，後者是透過簡訊。如果受害者真上了這些網路釣魚的當，威脅者將獲得他們 ETC 憑證以及儲存在 ETC 帳戶中的各種個人資料。除此之外，很多人可能在其他網路服務中使用相同密碼，然後威脅者可以嘗試存取這些服務。

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：

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)。

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。

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已於第一時間收錄於不安全分類列表中。

2022/08/03

Manjusaka 攻擊框架

根據最新報告，發現一個名為 Manjusaka 攻擊框架，正在真實網路環境大肆亂竄。Manjusaka 被威脅者以通常使用其他工具組合（例如：Cobalt Strike 或 Sliver）的替代品為宣傳噱頭，它使用基於 Rust 植入程式和採用 GoLang 編撰寫的二進位檔案。植入的惡意軟體具有各種功能，包括任意命令執行、對受感染終端的遠端遙控、檔案存取、憑證竊取等。Manjusaka 同時支援 Windows 和 Linux 平台，在攻擊鏈中所植入的惡意程式顯示出非常相似之功能。

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(Snoar)的防護：

- SONAR.SuspInject!g25
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt!gen9
- ISB.Downloader!gen136
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

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 373

基於安全強化政策(適用於使用DCS)：

賽門鐵克資料中心等級的重要主機防護系統：DCS(Data Center Security) 提供針對 Manjusaka 攻擊框架的零時差保護：

- 經 DCS 安全政策強化過的 Linux 伺服器可防止從 temp 或其他可寫入位置執行惡意軟體，該政策會拒絕將 nps.db 檔寫到磁碟上。
- DCS 安全政策強化還可以防止與 C&C 伺服器的所有入埠和離埠的連線。
- DCS 安全政策強化可防止來自外部網路的植入程式並防止下載有效籌載。

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。

2022/08/02

行動平台上的 DawDropper 植入程式，被利用於傳播銀行木馬病毒

DawDropper 是一個行動平台惡意軟體植入程式，偽裝成各種安卓軟體來進行傳播，例如：APP清理程式、文件掃描器、QR Code 掃描程式……等。該惡意軟體濫用 Firebase 即時資料庫--一個合法的協力廠商雲託管服務被濫用於 C&C 目的，還利用 GitHub 來託管惡意的有效籌載。據報導，DawDropper 已經傳播好幾個銀行木馬的變種，例如：Octo、Hydra、Ermac 和 Teabot。

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.1
- 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已於第一時間收錄於不安全分類列表中。

2022/08/02

HiddenAds--隱藏在 Google Play 商店中的全新惡意軟體家族

一種被稱為 HiddenAds 的新行動惡意軟體變體已被發現，它被偽裝成 Google Play 商店中的軟體移除程式。該惡意軟體在安裝後立即執行其惡意服務，使用者甚至不需要執行該應用程式。HiddenAds 會在受感染的設備上顯示各種廣告，包括彈跳視窗或覆蓋整個螢幕。據報導，傳播該惡意軟體的 APPs 在全球的下載量高達 100 萬次。

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已於第一時間收錄於不安全分類列表中。

2022/08/01

SilentCryptoMiner：偽裝成 chrome 的更新程式，利用瀏覽網頁時順道下載 (drive-by-download) 挖礦惡意程式

SilentCryptoMiner，顧名思義是一個加密貨幣挖礦惡意程式，能夠悄悄地挖掘各種貨幣，例如：乙太坊、Monero、Raptoreum……等。它通常會有一個被稱為 Unam 網頁面板，方便控制和命令在受害者機器上被執行的 SilentCryptoMiner。SilentCryptoMiner 和 Unam 都公開放在一個知名用於軟體開發和版本控制的網際網路代管平臺上，允許合法和非法使用。在過去幾週裡，賽門鐵克觀察到一個威脅者試圖透過瀏覽網頁時的順道下載攻擊 (drive-by-download) 來入侵機器，將挖礦惡意程式偽裝成 Chrome 瀏覽器更新程式以及遊戲駭客。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan Horse

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已於第一時間收錄於不安全分類列表中。

2022/07/29

被 KNOTWEED 駭客集團利用的 Subzero 惡意軟體

一個被稱為 Knotweed 威脅組織與世界各國的律師事務所、銀行和策略諮詢公司受到多起間諜軟體攻擊行動有關。威脅者一直利用被稱為 Subzero 的惡意軟體，它由兩個特定元件組成，名為 Jumplump 持續性載入程式和名為 Corelump 主要有效籌載。該惡意軟體透過 2021、2022 年各種攻擊行動，利用 Windows 和 Adobe Reader 中漏洞傳播。Subzero 允許攻擊者入侵目標電腦並透過遠程殼層 (remote shell) 執行相關命令和竊取各種機密資料，包括檔案、按鍵紀錄或螢幕截圖。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Mimikatz
- Trojan Horse
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

基於安全強化政策(適用於使用DCS)：

賽門鐵克資料中心等級的重要主機防護系統：DCS(Data Center Security) 內建的安全強化政策可有效防止 KNOTWEED 利用惡意軟體工具和有效籌載被安裝到 Windows 系統上。DCS 政策中的軟體安裝限制可以防止威脅用木馬化的二進位檔案篡改系統。DCS 安全強化政策還可以防止具有漏洞攻擊能力的下載程式連接到 C&C 伺服器下載任何有效籌載。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已於第一時間收錄於不安全分類列表中。