保安資訊--本周(台灣時間2022/07/29)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 98 萬 3,600 個受保護端點上總共阻止了1.689億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/07/24)**

- 在**19萬7,800**台端點上，阻止了**7,740萬**次嘗試掃描**Web**服務器的漏洞。
- 在**37萬5,500**台端點上，阻止了**3,750萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬2,800**台**Windows**伺服主機上，阻止了**2,050萬**次攻擊。
- 在**13萬7,000**端點上，阻止了**820萬**次嘗試掃描伺服器漏洞。
- 在**6萬8,600**台端點上，阻止了**330萬**次嘗試掃描在**CMS**漏洞。
- 在**10萬3,800**台端點上，阻止了**320萬**次嘗試利用的應用程式漏洞。
- 在**30萬4,100**台端點上，阻止了**820萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7萬2,000**台端點上，阻止了**390萬**次加密貨幣挖礦攻擊。
- 在**41萬4,000**台端點上，阻止了**610萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,300**台端點上，阻止了**19萬6,600**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。

2022/07/27

惡意軟體 RelicRace／RelicSource 搭檔，被利用來傳遞 Formbook 和 Snake 鍵盤側錄程式

在真實網路環境觀察到一個以 TGZ 格式壓縮檔為附件的新惡意軟體攻擊行動。這個 TGZ 壓縮檔內包含一個可執行檔，被認定為基於 .NET 的下載程式：RelicRace，其目的是在被攻擊的系統上下載和執行惡名昭彰的 RelicSource 惡意軟體。這些可執行檔在受感染的電腦上下載並安裝 Formbook 惡意軟體和 Snake 鍵盤側錄程式作為最終的有效籌載。Formbook 惡意軟體從受害者的設備中竊取個人資訊，並使用來自 C&C 伺服器的控制命令和 Snake 鍵盤側錄程式操縱這些系統，以竊取並匯出敏感性資料，包括使用者憑證、剪貼簿資料、鍵盤輸入記錄及其他惡意行為。

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：

- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Formbook
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2022/07/26

AMEXTROLL 安卓網路銀行惡意軟體

名為 AMEXTROLL (也被稱為 Brata) 的安卓網路銀行惡意軟體在真實環境到處流竄，並在地下論壇上大肆宣傳，以每月 3,500 美元的價格出租。據報導，一個威脅發動者一直透過釣魚網站鎖定安卓平台使用者為目標，並將其偽裝成一個安全應用程式 APP -- 這是最近在行動威脅領域常見的社交工程手法。

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。

- 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。

2022/07/25

Luca Stealer -- 一個全新的 Rust 語言竊密程式

一個用 Rust 程式設計語言撰寫、被稱為 Luca Stealer 的全新竊密程式已被發現。這個惡意軟體原始程式碼最近在一個網路犯罪論壇上被洩露。該惡意軟體主要針對基於 Chromium 的瀏覽器、訊息應用程式和加密錢包，並增加竊取受害者檔案的功能。該竊密程式具有木馬的功能，能透過 Telegram 機器人或 Discord 的 webhooks 資料拋接將搜集彙整後的資料、憑證或財務資訊洩漏轉移出去。

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：

- Downloader
- Trojan Horse
- Trojan.Gen.MBT
- 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 564
- System Infected: Trojan.Backdoor Activity 634

2022/07/24

Candiru 間諜軟體

Candiru 間諜軟體在 2021 年 7 月首次被發現，並在幾個月內銷聲匿跡。本月初，發現它利用最近被發現 Chrome 瀏覽器零日漏洞 (CVE-2022-2294) 來發動攻擊，主要目標是中東的記者。

在漏洞利用得逞後，一個名為“Devil's Tongue* 魔鬼之舌”的惡意有效籌載將被植入。其功能包括從 LSASS、Chrome 和 Firefox ……等瀏覽器中竊取受害者的憑證、採集檔案、登錄機碼偵查、執行 WMI 命令以及查詢 SQLite 資料庫。

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：

- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22

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。

2022/07/22

新版 GoMet 後門針對烏克蘭的組織

在針對烏克蘭組織的攻擊行動中發現 GoMet 後門的新變種。顧名思義，GoMet 是用 Go 程式語言撰寫的，包括遠端命令執行和檔案上傳／下載功能。該惡意軟體能夠執行預先排定的 cron 工作排程作業，來確保與攻擊者的 C&C 伺服主機的持續連接。

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

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。

2022/07/21

Lightning 框架，對 Linux 平台的嚴重威脅

隨著越來越多的犯罪活動被曝光，Linux 的威脅形勢日益猖獗。Lightning 框架是最新，它可以透過核心模組中的外掛來部署後門和 rootkit。據報導，這種威脅會脫穎而出，主因是 Linux 平台上的惡意軟體向來很少如此精密老練。Lightning 框架背後的攻擊者一直使用 Typosquatting 手法(利用相似域名的詐騙)，將他們惡意二進位檔案偽裝成已知的軟體，例如： Seahorse。

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

基於安全強化政策(適用於使用DCS)：

賽門鐵克 DCS 的安全強化政策採用的安全技術，完全依循 MITRE Boot 或 Logon 初始語法，可有效防止 Lightning 框架惡意軟體感染 Linux 主機以及避免建立持久性。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。