保安資訊--本周(台灣時間2022/05/20)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 120 萬個受保護端點上總共阻止了1.967億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/05/19)**

- 在**22萬800**台端點上，阻止了**1億550萬**次嘗試掃描**Web**服務器的漏洞。
- 在**44萬5,600**台端點上，阻止了**3,760萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬1,900**台**Windows**伺服主機上，阻止了**2,250萬**次攻擊。
- 在**16萬2,700**端點上，阻止了**990萬**次嘗試掃描伺服器漏洞。
- 在**8萬3,300**台端點上，阻止了**420萬**次嘗試掃描在**CMS**漏洞。
- 在**13萬5,400**台端點上，阻止了**390萬**次嘗試利用的應用程式漏洞。
- 在**36萬9,400**台端點上，阻止了**960萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,710**台端點上，阻止了**370萬**次加密貨幣挖礦攻擊。
- 在**11萬8,100**台端點上，阻止了**540萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,100**台端點上，阻止了**22萬1,000**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。

2022/05/17

鎖定德國的客製化 PowerShell 遠端存取木馬 (RAT)

最近發現一個以德國作為目標，利用俄羅斯和烏克蘭之間正在發生的衝突，作為誘餌的惡意軟體行動。據稱，該檔案假借包含烏克蘭當前最新局勢狀態，而實際上它包含一個遠端存取木馬（RAT）有效籌載，來進行後門運作，對受害者的電腦進行管理控制。

該遠端存取木馬會執行以下指令：

- **Download** (type: D0WNl04D)：從伺服主機下載檔案
- **Upload** (type: UPL04D)：上傳檔案到伺服主機
- **LoadPS1** (type: L04DPS1)：載入並執行PowerShell 腳本
- **Command** (type: C0MM4ND)：執行特定的指令

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan Horse
- WS.Malware.1
- 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已於第一時間收錄於不安全分類列表中。

2022/05/16

越來越多遭入侵的 WordPress 網站將瀏覽者重新導向到廣告網站

多年來，WordPress 受歡迎程度一直屹立不搖，到今天為止，網路上大量的網站都是架構在這個開放原始碼的內容管理系統上。這種盛況不可避免地使它成為網路犯罪覬覦的主要目標，而且威脅者每天都在不斷入侵有漏洞的 WordPress 網站。大多數遭入侵的 WordPress 網站通常最終被變成廣告、網路釣魚和惡意軟體的重新導向平臺。最近，有更多關於 WordPress 網站被注入惡意的 javascript，將瀏覽者重新導向到不同網域的報導。

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
- Web Attack: Mass Injection Website 91
- Web Attack: Unwanted Browser Notification Website 29
- Web Attack: Unwanted Browser Notification Website 30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- MSIL.Downloader!gen8

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。

2022/05/15

惡意垃圾郵件行動引發 SYK Crypter 加密程式的氾濫

最近，一個基於 .NET 加密程式（SYK）消息被曝光，該加密程式被威脅者利用，作為他們針對各種組織的惡意垃圾郵件行動之兩階段攻擊鏈的一部分。如果受害者成功地被他們常用的社交工程騙術報價和訂單所引誘，惡意附件（一個 .Net 載入程式）將下載一個託管在 Discord 的加密資料。然後，它將被解密為 SYK 加密程式，其作用就是載入到遭入侵電腦的記憶體中並解密最終有效籌載。根據報告，已經看到多個已知和常見的有效籌載，包括 Nanocore、Redline 竊密軟體、Quasar 遠存取木馬等。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- MSIL.Downloader!gen8

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/05/13

Eternity Project (*永恆專案) 提供各種惡意軟體出售，通過 Telegram (簡稱TG) 做廣告

威脅者正在經營一個新的惡意軟體即服務業務，該業務被稱為 Eternity Project (*永恆專案)，並透過 Telegram 進行宣傳。

Eternity 惡意軟體是模組化的工具包，提供竊密軟體、挖礦程式、加密錢包／貨幣竊取程式、勒索軟體程式和蠕蟲傳播器的銷售，這些都可以個別購買，價格不等，從 90 美元的挖礦程式到 490 美元勒索軟體。營運商顯然還計畫很快提供一個分散式拒絕服務 (DDoS) 機器人。

這個工具包幕後的威脅者，正在透過一個擁有約 500 名訂閱者的 Telegram 頻道來推廣它，他們在那裡分享惡意軟體的最新資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C