保安資訊--本周(台灣時間2023/04/14)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 73 萬 4,400 台受保護端點上總共阻止了 8,780 萬次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2023/04/10)**

- 在**14萬6,100**台端點上，阻止了**3,600**萬次嘗試掃描**Web**服務器的漏洞。
- 在**26萬200**台端點上，阻止了**1,840**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬4,000**台**Windows**伺服主機上，阻止了**1,540**萬次攻擊。
- 在**8萬1,800**台端點上，阻止了**260**萬次嘗試掃描伺服器漏洞。
- 在**1萬6,100**台端點上，阻止了**90萬4,000**次嘗試掃描在**CMS**漏洞。
- 在**5萬6,600**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**24萬6,200**台端點上，阻止了**470**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3萬4,000**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**14萬6,700**台端點上，阻止了**1,090**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,400**台端點上，阻止了**10萬2,200**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。

2023/04/13

報稅季節請小心～以報稅協助為幌子的惡意行動散佈GuLoader惡意程式

GuLoader 是漏洞利用 shellcode 類型的惡意下載器，已知可以載入或注入各種不同的惡意軟體，包括勒索軟體、竊密程式、銀行木馬、遠端存取木馬 (RAT) 等。在網路上觀察到一項利用報稅協助為幌子來誘騙下載 GuLoader 有效酬載惡意行動。報稅相關的誘餌在報稅期間是非常熱門的詐騙幌子，每年都有不同的威脅攻擊者使用這種伎倆，來傳播惡意軟體和竊取機密資料。在最近的惡意攻擊行動中，攻擊者利用帶有密碼保護 .zip 壓縮檔下載鏈結的惡意垃圾郵件。下載解縮壓後，受害者會取得偽裝成 .pdf 檔的捷徑檔，這些檔案依次呼叫 PowerShell 指令以從遠端位置取得高度混淆的 Visual Basic 惡意腳本。

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Scr.Malcode!gen36
- VBS.Downloader.Trojan
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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。

2023/04/12

Hydra行動竊密程式持續偽裝成Google Play商店

Hydra 出現在行動威脅領域已有一段時間，而且行跡遍步全球。最近觀察到多個登入頁面，其中有駭客組織和個體戶將 Hydra 偽裝成 Google Play 商店（一種慣用伎倆）。當手機用戶被誘騙下載和安裝 Hydra 時，它有能力執行一系列有害的操作。這些行為包括收集敏感資訊，例如：聯絡人、手機簡訊內容、竊取 cookie、注入／覆蓋金融APP，以及攔截一次性密碼 (OTP)、裝置個人識別碼 (PIN) 和其他有價值的資料。

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：

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

2023/04/12

Trigona勒索軟體～專門鎖定MS SQL伺服器

Trigona 是一種勒索軟體變種，最初發現於 2022 年。據報導，該惡意軟體與 CryLock 勒索軟體有一定的相似之處。Trigona 最近被用來針對易遭受攻擊或配置與設定錯誤 SQL 伺服器的攻擊。攻擊者在攻擊的初始階段部署 CLR Shell 惡意軟體，其被用來做為權限提升和收集系統資訊的漏洞利用開採工具。被其加密後檔案將被新增 ._locked 的副檔，並在每個被加密檔的資料夾中置放檔名為“how_to_decrypt.hta”網頁格式檔的勒索贖金說明。

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.Cryptlck!g171
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Cryptolocker
- Ransom.Trigona
- Ransom.Trigona!g1
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/04/11

駭客購買搜尋引擎最佳化(SEO)廣告，將受害者重導向曖昧的成人約會和色情網站

購買搜尋引擎最佳化 (SEO) 廣告攻擊 (也有人稱搜尋引擎最佳化下毒)，在這幾個月成為頭條新聞，也發現更多這類型的惡意行動。這種類型的攻擊方式包含操縱搜索引擎結果來誤導使用者瀏覽惡意網站或網站組，以惡意軟體感染使用者電腦、以釣魚網站誘騙他們的帳密或引誘他們掉落駭客所操縱的詐騙計劃。

賽門鐵克最近觀察到 SEO 下毒行動，使用者會被透過具有開放或易受攻擊的正常網站重導向到成人網站（色情和約會）。搜索引擎回應的查詢字符中包含似是而非的網址字串（已發現其中數千個）。

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：

- URL reputation: Browser navigation to known bad URL

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)：

- 觀察到的站台已列入在網頁安全類別清單中
- 賽門鐵克的WebPulse網頁安全生態系統，為新出現的網頁提升風險級別
- 新出現的網頁將會依網站內容和監控數據的規則第一時間就進行分類

2023/04/11

兩年前揭露Log4j漏洞，現在還常被利用來發動代理劫持攻擊

CVE-2021-44228（又名 Log4Shell）是 Apache Log4j 日誌框架中的一個嚴重漏洞，早在 2021 年就已公開揭露。儘管該漏洞已經為人所知兩年，但仍經常在網路上被開採利用。根據最近一份報告，一項全新行動利用 CVE-2021-44228 漏洞來進行代理劫持。在威脅攻擊者獲得對此類攻擊中目標端點的存取權限後，他們會安裝一個惡意代理程式，成功地將遭駭的系統轉換為遠端代理伺服器。攻擊者可透過將此受感染伺服器的存取權限出售給代理軟體服務提供商來獲利。

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

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: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j2 RCE CVE-2021-44228 3
- Attack: Log4j2 RCE CVE-2021-44228 4
- Attack: Log4j2 RCE CVE-2021-44228 5
- Attack: Log4j2 RCE CVE-2021-44228 7

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。

2023/04/11

Cylance勒索軟體同時針對Windows和Linux平台

Cylance 是一種新發現的勒索軟體，它可以同時針對 Windows 和 Linux 的系統。該惡意軟體的 Windows 變種建立一個名為“CylanceMutex”程序鎖（mutex），以確保只有一個有效籌載實例在受感染的機器上執行，被其加密後的檔案會被新增 .Cylance 副檔名。成功加密後，惡意軟體會以“CYLANCE_README.txt”文字檔的形式留下勒索贖金說明。Cylance 勒索軟體可常駐在環境裡和刪除受感染端點上的刪除陰影複製 (shadow copies) 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(SONAR)的防護：

- SONAR.Ransom!gen98
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g12
- SONAR.Ransomware!g28

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Ransom.Generic.1
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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：

- System Infected: Bad Reputation Process Request 4
- System Infected: Trojan.Backdoor Activity 634

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。

2023/04/10

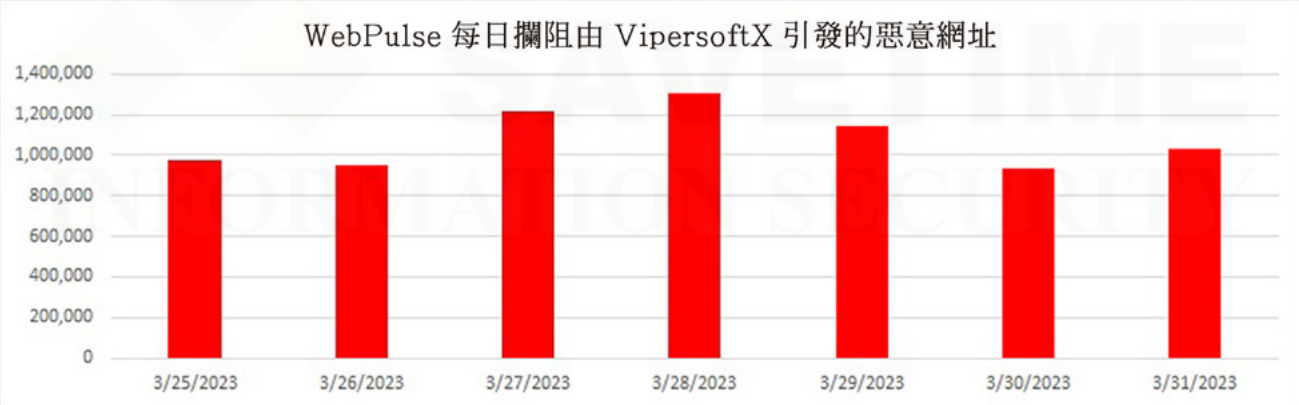
防護亮點：賽門鐵克WebPulse網頁安全生態系統，每天偵測到由VipersoftX觸發的百萬次惡意網址連結，為用戶提供更高層級的保護

～防護亮點～

VipersoftX 是一種相當詭異的竊密惡意軟體，至少從 2019 年底開始就存在。它一種經過高度混淆並定期更新的遠端存取木馬 (RAT)，透過使用破解的軟體經由世界各地的種子 (torrents) 和軟體共享站台進行傳播。最近觀察到它部署為隱藏的小型 PowerShell 腳本在大型系統檔中試圖避免檢測。它主要目標是竊取加密貨幣，採用諸如剪貼簿置換、主機數位指紋識別以及將其他惡意籌載下載到受感染電腦上等技術。

較新版本 ViperSoftX 包含用於安裝瀏覽器擴充元件的有效籌載，該擴充元件有效地為其提供對受害者瀏覽每個頁面的存取權限，使其能夠對瀏覽器發動中間人攻擊來執行加密貨幣錢包地址置換並竊取憑證以及其他剪貼板內容。它透過檢查剪貼簿的內容來竊取加密貨幣，比對是否持有與加密貨幣錢包地址匹配的特徵。如果找到匹配的特徵，它會用自己的錢包地址覆蓋剪貼簿內容。這些方法，簡單但有效。

賽門鐵克 WebPulse 網頁安全生態系統，長期以來一直專注在檢測並阻止來自 VipersoftX 散布惡意瀏覽器擴充元件的大量流量。平均每天有超過一百萬個 URL 請求。



惡意瀏覽器外掛會生成大量 DGA 網域產生演算法生成惡意軟體搭配 C&C 伺服器域名與 IP 位址的虛假網域，這些網域會出現在我們客戶的網頁流量中。在其廣泛的武器庫中，WebPulse 有為數眾多的先進“殭屍網路流量檢測機制”，其中一些會自動觸發此流量。賽門鐵克客戶可以在他們的日誌中使用這些 WebPulse 檢測（被歸類的網頁類別是“惡意離埠數據／殭屍網路”）快速找出他們組織內發送此惡意流量的電腦。

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 **零時差**防護技術偵測到的惡意程式名稱及有效對應的防護機制：

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)：

被歸類的網頁類別：惡意離埠數據／殭屍網路。

要了解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。

2023/04/10

Rilide竊密程式偽裝成的瀏覽器擴充功能進行惡意活動

最近發現一種被稱為 Rilide 竊密程式偽裝成 Chrome 瀏覽器擴充功能進行惡意活動。Rilide 偽裝成合法的瀏覽器擴展來發動惡意行動，例如：腳本注入、螢幕截圖或從各種交易所竊取加密貨幣。首次部署 Rilide 呼叫或下載等載入程序時，它會修改瀏覽器的快捷列內容，以便在啟動瀏覽器時額外執行一個參數，該參數指向先前已遭入侵的電腦系統上植入的惡意擴充。Ekipa 遠端存取木馬 (RAT) 和 Aurora 竊密程式等惡意軟體家族，最近被用來傳播 Rilide 竊密程式。

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!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Malscript
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

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／IP位址已於第一時間收錄於不安全分類列表中。