保安資訊--本周(台灣時間2022/06/03)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 110 萬個受保護端點上總共阻止了1.997億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/05/30)**

- 在**21萬7,600**台端點上，阻止了**1,004萬**次嘗試掃描**Web**服務器的漏洞。
- 在**42萬4,900**台端點上，阻止了**3,970萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬7,200**台**Windows**伺服主機上，阻止了**2,200萬**次攻擊。
- 在**15萬8,200**端點上，阻止了**950萬**次嘗試掃描伺服器漏洞。
- 在**8萬2,000**台端點上，阻止了**400萬**次嘗試掃描在**CMS**漏洞。
- 在**11萬9,200**台端點上，阻止了**380萬**次嘗試利用的應用程式漏洞。
- 在**36萬1,100**台端點上，阻止了**900萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**820**台端點上，阻止了**350萬**次加密貨幣挖礦攻擊。
- 在**11萬4,100**台端點上，阻止了**540萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,600**台端點上，阻止了**20萬6,500**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。

2022/06/03
中國駭客集團：LuoYu，濫用新技術傳播 WinDealer 惡意軟體

中國的進階持續威脅 (APT) 組織：LuoYu 被觀察到濫用一種新的「旁觀者」(man-on-the-side) 攻擊技術，傳播 WinDealer 惡意軟體來感染使用者。透過監控網路的常見流量，例如：應用程式更新，他們用惡意的有效籌載取代有效回覆。WinDealer 獨特之處在於，它將透過一大批隨機 IP 位址連接到命令和控制伺服器 (C&C)，而不是其他攻擊更常使用的預先設定好的硬編碼位址，這使得它更難被攔截。一旦被安裝，將允許攻擊者竊取資料、編輯檔案、安裝後門和掃描網路。

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
- Trojan.Gen.2
- Trojan.Gen.NPE
- W97M.Downloader
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/06/03
SiMay 遠端存取木馬 (RAT) 在濫用雲端服務的攻擊中被傳播

SiMay 遠端存取木馬 (RAT) 在最近一次濫用雲端服務的行動中傳播。攻擊鏈包含多階段的下載器二進位檔案，這些二進位檔案獲取含惡意 .dll 檔的 .zip 檔案。有效載荷 dlls 透過 DLL 側載技術被載入到記憶體中。據報導，最新 SiMay 變種還利用一個早在 2018 年 WinRAR 存在的漏洞，以便在被攻擊的機器上建立以實現其持續性。

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
- Trojan.Gen.2
- Trojan.Gen.MBT
- Ws.Malware.1

基於行為偵測技術(Snoar)的防護：

- SONAR.Heur.RGC!g542
- SONAR.SuspBeh!gen6
- SONAR.SuspBeh!gen633

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：

- 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。

2022/06/02

AtomBot 發動的分散式阻斷 (DDOS) 攻擊行動

AtomBot 惡意軟體在最近行動中利用 GitLab 遠端命令執行 (RCE) 漏洞 (CVE-2021-22205) 進行散佈。在利用這一漏洞後，被入侵的系統將被特有惡意二進位檔案所控制，並能連接到 C&C 伺服器以獲得攻擊者的進一步指令。AtomBot 主要用於發動分散式阻斷 (DDOS) 攻擊行動。

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
- Linux.Mirai
- 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：

- Attack: GitLab CE CVE-2021-22205 RCE

2022/06/02

Clipminer 殭屍網路

賽門鐵克的威脅獵手團隊 (隸屬 Broadcom--博通軟體事業部的企業安全部門) 發現一個網路犯罪行動，該行動背後的行為者可能從加密貨幣挖礦和通過剪貼簿劫持 (clipboard hijacking) 進行盜竊中獲得至少 170 萬美元的非法收益。正在使用的 Clipminer 惡意軟體與另一個名為 KryptoCibule 的加密貨幣挖礦木馬有許多相似之處，這表明示它可能是該威脅的模仿者或演變者。Clipminer 有能力利用被入侵的電腦資源來挖礦。該惡意軟體還修改剪貼簿內容，試圖重新轉向受感染電腦使用者的加密貨幣交易。

在我們的部落格有更多詳細資訊 -- Clipminer (*剪貼礦工)：殭屍網路的營運商從中獲利超過$170萬美元。

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.Clipminer
- Trojan.Gen.MBT
- WS.Malware.1

2022/05/31

Follina -- 微軟支援診斷工具 (MSDT) 的遠端程式碼執行漏洞 (CVE-2022-30190)

已有報告指出，一個被稱為 Follina 的漏洞，它允許微軟 Office 文件檔 (例如：Word) 開啟一個惡意的網址 (URL)，並透過微軟支援診斷工具（MS Support Diagnostic Tool：MSDT）中的遠端程式碼執行漏洞（CVE-2022-30190）啟動攻擊鏈--該工具為微軟支援部門收集資訊。到目前為止，已經發現幾個流竄在外的真實樣本，概念證明已經公開發佈。我們應該預期會有更多的威脅者利用這個漏洞的嚴重性。

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
- Trojan.Mesdetty
- W97M.Downloader

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。

基於安全強化政策(適用於使用DCS)：

DCS 預設政策就有針對 MS Office 應用程式特別作安全強化。DCS 防止MS Office 應用程式啟動命令解譯器，包括 cmd.exe、powerhell.exe 和其他子程序。此外，對於這個編號的漏洞，可以透過將 *\msdt.exe 新增到沙箱執行控制 "Microsoft Office不可執行的程式" 中來防止遠端程式碼執行漏洞。

2022/05/27

攻擊行動用戶的新 Android (*安卓) 遠端存取木馬 (RAT)

一個針對行動用戶傳播 Android (*安卓) 遠端存取木馬 (RAT) 新攻擊行動已在網路上流竄。這些惡意軟體樣本使用各種合法公司和應用程式的名稱和圖示，例如：Google.apk、Google Service Framework.apk、ZeniTevi.apk 等。該行動遠端存取木馬 (RAT) 試圖竊取使用者資料、簡訊、通話記錄和有關被攻擊設備本身的資訊。該惡意軟體還具有錄音／錄影和拍照的功能。

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：

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。

- Android.Reputation.1
- Android.Reputation.2
- AppRisk:Generisk