保安資訊--本周(台灣時間2023/10/06)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 66 萬 1,700 台受保護端點上總共阻止了 8,250 萬次攻擊。這些攻擊中有 87.4% 在感染階段前就被有效阻止：**(2023/10/03)**

- 在**14萬4,500**台端點上，阻止了**3,540**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**21萬2,100**台端點上，阻止了**1,530**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬7,100**台**Windows**伺服主機上，阻止了**1,490**萬次攻擊。
- 在**8萬7,700**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,000**台端點上，阻止了**99萬8,800**次嘗試掃描在**CMS**漏洞。
- 在**8萬600**台端點上，阻止了**170**萬次嘗試利用的應用程式漏洞。
- 在**22萬5,400**台端點上，阻止了**450**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3,000**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**13萬5,600**台端點上，阻止了**840**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**934**台端點上，阻止了**7萬4,100**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。

2023/10/04

Chaos勒索軟體覬覦講法語《創世神：Minecraft》的玩家

Minecraft 是一款風靡全球的線上遊戲，許多網路犯罪分子利用它的風靡而瞄準它的玩家社群。在最近一個例子中，賽門鐵克觀察到一個 Chaos 勒索軟體威脅者將其惡意檔案偽裝成 Minecraft 安裝程式，引誘講法語的玩家下載。一旦加密成功，它就會留置法語的贖金支付說明，要求在 72 小時內支付 0.006 比特幣的贖金（撰寫本文時價值 166.12 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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen625

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/10/04

Capybara竊密程式

賽門鐵克發現一個與 Capybara 竊密程式有關聯的命令控制伺服器 (C&C)，該竊密程式目前正在 Telegram 和 Discord 上推廣。

如果使用者被成功誘騙執行 Capybara，惡意軟體首先會檢查它是否在虛擬機器 (VM) 內運行。如果不是，它隨後會嘗試終止以下處理程序 (Process)：『httpdebuggerui』、『wireshark』、『fiddler』、『vboxservice』、『df5serv』、『processhacker』、『vboxtray』、『vmtoolsd』、『vmwaretray』、『ida64』、『ollydbg』、『pestudio』、『vmwareuser』、『vgauthservice』、『vmacthlp』、『x96dbg』、『vmsrvc』、『x32dbg』、『vmusrvc,』、『prl_cc』、『prl_tools』、『xenservice』、『qemu-ga』、『joeboxcontrol』、『ksdumperclient』、『ksdumper』和『joeboxserver』。

Capybara 具有以下功能：

- 螢幕截圖並在指定螢幕上執行滑鼠點擊。
- 鍵盤側錄。
- 收集電腦資訊、網路配置細節、已安裝的程式、處理程序清單、FileZilla 伺服器資訊、Discord 備份代碼、遠端桌面連接、各種虛擬幣應用程式和擴展錢包的錢包、Discord 和瀏覽器的權杖以及瀏覽器資料（cookie、歷史記錄、書簽、表格自動填充和密碼）。
- 停用指定 PID 的處理程序。
- 下載、檢索或刪除檔案。

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.Maljava

2023/10/04

Progress軟體發布最嚴重等級的WS_FTP伺服器漏洞警告

Progress 軟體公司是 MOVEit Transfer 檔案分享平臺的製造商，該平臺最近在廣泛的資料盜竊攻擊中被利用，該公司正就其 WS_FTP 伺服器軟體中一個最嚴重等級的漏洞向客戶發出警告。

Progress 公司披露影響該軟體管理器介面和臨時傳輸模組的多個漏洞。其中兩個漏洞被評為嚴重，一個漏洞（CVE-2023-40044）被評為最高 10/10 嚴重等級。CVE-2023-40044 允許未經認證的攻擊者在成功利用 Ad Hoc Transfer 模組中的 .NET 反序列化漏洞後執行遠端命令。另一個嚴重等級的漏洞 (CVE-2023-42657) 是一個目錄遍歷漏洞，攻擊者可利用該漏洞在授權的 WS_FTP 資料夾路徑之外執行檔案操作。

開採利用這兩個漏洞，惡意威脅者可以逃離 WS_FTP 伺服器檔案結構的上下文，並在底層作業系統上執行檔案操作。這兩個漏洞都可以在不需要任何使用者交互的低複雜度攻擊中被利用。

Progress 建議用戶全面升級到最新版本，以修復該問題。

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：

基於安全強化政策(適用於使用DCS)：

賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：其出廠就內建的強化政策就能完全提供零時差攻擊保護，防止利用遠端程式碼執行 (RCE) 和檔案遍歷漏洞（例如：WS_FTP 伺服器中的 CVE-2023-40044 和 CVE-2023-42657）的威脅。DCS 內建的 sym_win_hardened_sbp 強化規則可防止在伺服器上執行任意命令以及篡改關鍵作業系統檔案和資料夾。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/10/04

針對NPM平臺的誤植域名(打錯字)攻擊行動

發現一個針對 NPM 平臺的誤植域名 (打錯字) 攻擊行動 (NPM：Node Package Manager 的縮寫，是 Node.js 預設的 node 套件管理平台，簡單來說可以當作是一個建立跟管理專案的好用套件，也可以下載好用的工具，該平臺是一個軟體發展人員常常參考使用的的開源工具庫。威脅者只需在合法套裝軟體『node-hide-console-window』上添加字母『s』，就能將其變成惡意套裝軟體『node-hide-console-windows』。據報導，該模組提供一個名為『r77』的 rootkit，它與開源惡意軟體 DiscordRAT 2.0 有相關聯。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2023/10/04

數百萬台Exim郵件伺服主機遭受遠端攻擊

Exim 郵件傳輸代理 (MTA) 中的一個嚴重等級漏洞可讓未經認證的攻擊者在目標系統上執行惡意程式碼。(網路上的註解：Exim 是劍橋大學開發的郵件傳送代理程式 (Mail Transfer Agent，MTA)，主要安裝在 Linux 系統以作為郵件伺服器。)

該漏洞 (CVE-2023-42115) 早在 2022 年 6 月就被發現，並通過趨勢科技的『零日計畫』(ZDI) 被披露。而雖然該漏洞在 2022 年 6 月提報給 Exim 團隊，並在 2023 年 5 月再次被提報，但開發人員未能提供修補進度的更新。於是，ZDI 決定於 2023 年 9 月 27 日發佈關於該漏洞的公告。

CVE-2023-42115 存在於 SMTP 服務中，該服務預設監聽 TCP 埠 25。該漏洞存在的原因是對使用者提供的資料驗證不充分，可能導致寫入超過緩衝區的末端。

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：

基於安全強化政策(適用於使用DCS)：

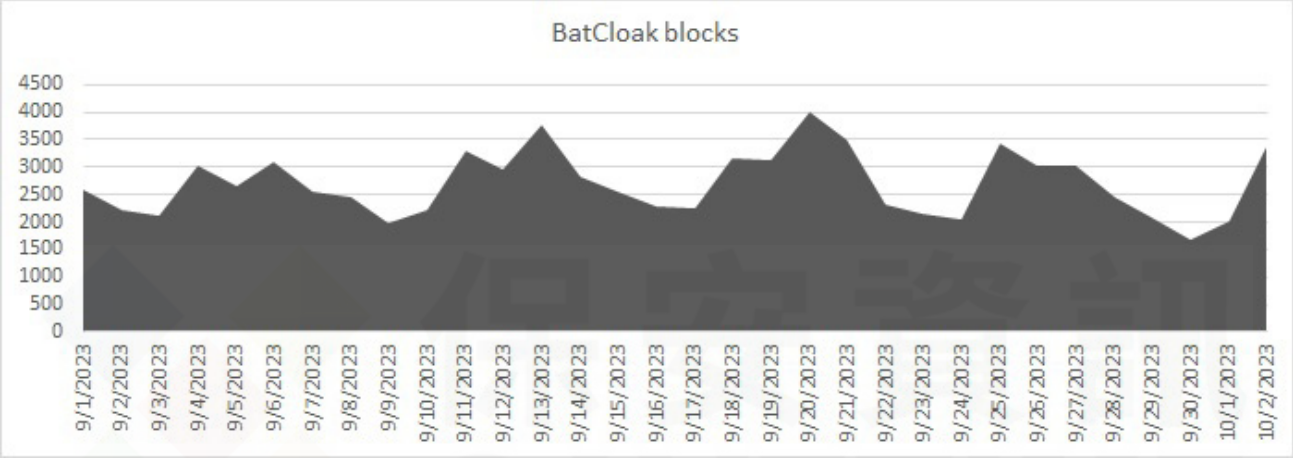
賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：其出廠就內建的 sym_unix_protection_sbp 強化規則已內建的最少權限、最低資源的沙箱運行環境，同時支援最多種主流 Linux 平台。預設就啟動的多層次政策鎖定控制功能，可防止威脅者在 Exim 伺服器上執行任意命令以及篡改關鍵作業系統檔案和資料夾。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/10/03

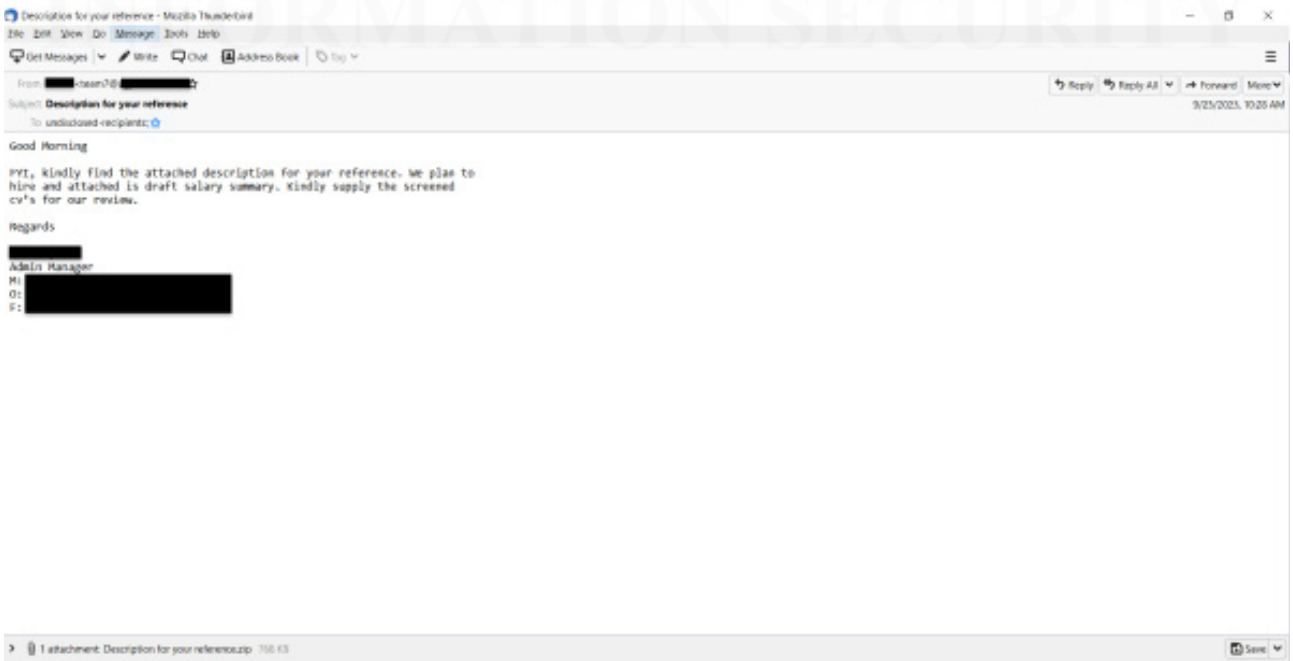
防護亮點：BatCloak 使威脅形勢雪上加霜

.BAT 的批次檔由於其簡單性、也是 Windows 內建的功能、容易隱藏的特性和具有腳本編寫功能…等，長期以來一直被網路上的壞蛋用於各種目的，但主要還是用作惡意程式載入程式。

就在幾個月前，一種被稱為 BatCloak 的批次檔混淆工具引起安全研究人員的關注，多份報告顯示惡意批次載入程式被該工具混淆，並在世界各地的攻擊行動中用於傳遞惡意籌載，例如：資訊竊取程式、遠端存取木馬等。賽門鐵克安全產品截至 9 月記錄的偵測顯示，正在發生相當一致的攻擊浪潮。



賽門鐵克最近觀察到一名冒充印度人力資源公司的參與者，主要向工程、酒店和零售業提供人力資源服務。惡意電子郵件被偽裝成人力招募優惠發送世界各地的公司和政府機構。該附件偽裝成履歷，採用 zip 壓縮檔的形式，其中包含一個 bat 檔案 (參考說明.zip＞參考說明.bat)。



如果毫無戒心的用戶下載該批次檔並執行，他們實際上將執行 Agent Tesla--一個惡名昭彰且非常熱門的竊密程式，我們已多次在此發布。

賽門鐵克的多重防護技術已經於第一時間提供最有效的護(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.BatCloak!gen1
- SONAR.BatCloak!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.BatCloak
- Trojan.BatCloak!gen1
- Trojan.BatCloak!gen2

欲深入了解更多有關於賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

2023/10/02

Menorah，Crambus所為的新惡意軟體 (APT34)

進階持續性威脅 (APT) 組織：Crambus (又稱 OilRig、APT34) 是一個主要集中在中東的秘密網路間諜組織，透過魚叉式網路釣魚行動收集敏感情報。該組織發現一種全新的惡意軟體，名為 Menorah。該惡意軟體透過惡意 offce 檔案進行散播，該檔案負責下載惡意軟體並建立排程任務以在後台運行它。Menorah 可以被認為是一個後門，具有收集系統資訊、下載和上傳檔案到系統以及執行 shell 命令的功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Ratenjay
- ISB.Downloader!s442
- W97M.Downloader
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。