保安資訊--本周(台灣時間2023/03/10)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 82 萬 2,500 台受保護端點上總共阻止了 9,560 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/03/06)**

- 在**16萬2,500**台端點上，阻止了**3,540**萬次嘗試掃描**Web**服務器的漏洞。
- 在**29萬6,400**台端點上，阻止了**2,240**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬9,400**台**Windows**伺服主機上，阻止了**1,610**萬次攻擊。
- 在**9萬2,800**台端點上，阻止了**290**萬次嘗試掃描伺服器漏洞。
- 在**1萬9,700**台端點上，阻止了**110**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬8,600**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**27萬2,700**台端點上，阻止了**570**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3萬1,000**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**15萬300**台端點上，阻止了**1,2100**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,900**台端點上，阻止了**18萬6,000**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。

2023/03/09

MedusaLocker勒索軟體仍活耀在真實網路環境

MedusaLocker 是 2019 年底首次發現全新的勒索軟體，顯示出與另一個被稱為 GlobeImposter 勒索軟體有些淵源。MedusaLocker是一種勒索軟體即服務 (RaaS) 的惡意軟體，已知其利用遠端桌面協定 (RDP) 的漏洞來存取目標網路。在上個月，健康產業網路安全協調中心 (HC3) 發佈一個警告，警告與 MedusaLocker 有關的威脅者可能會針對醫療部門進行攻擊。MedusaLocker 在加密的檔案中新增各種不同的副檔名。最近發現這種勒索軟體之變種所使用一些副檔名的例子包括。.allock、.filesencrypted、.lockfiles、.marnet2、.onelock和.skynetwork8。

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：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g18
- SONAR.UACBypass!gen30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Cryptolocker
- Ransom.Globeimposter
- Ransom.Locky!g35
- Ransom.MedusaLocker
- WS.Malware.1
- WS.SecurityRisk.4

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

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: Ransom.Gen Activity 56

2023/03/09

白色剛走，黑蛇就來～源於Chaos的變種勒索軟體：BlackSnake(*黑蛇)

BlackSnake 是一個源於 Chaos 程式碼的新變種勒索軟體。除了最常見的勒索軟體功能外，BlackSnake 還含剪貼簿竊密器 (Clipper) 模組，使其能夠竊取加密貨幣錢包。在竊取資料後，該勒索軟體將會進行檔案加密，並新增 .pay2unlock 的副檔名。BlackSnake 將根據預先定義的排除清單避免加密特定的系統相關資料夾和檔案，以防止系統不穩定而在檔案加密過程中遭用戶起疑。

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：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g22

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

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

2023/03/09

親巴基斯坦國家級駭客集團--Transparent Tribe，誘騙行動手機用戶安裝CapraRAT遠端存取木馬程式

在真實網路環境觀察到一起歸因於 Transparent Tribe 駭客集團的新活動。該攻擊行動主要針對來自印度和巴基斯坦的行動手機用戶，並散布稱為 CapraRAT 的遠端存取木馬程式。該惡意軟體被偽裝成訊息／撥號手機 APP，可以從被入侵的裝置中竊取機敏的使用者的資訊。CapraRAT 具有螢幕擷取、錄音、查看通話記錄、下載檔案、發送文字訊息和撥打電話等功能。

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

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。

2023/03/08

Rever勒索軟體，偶爾也會有較大的行動來喚起大家的記憶

Rever 勒索軟體在威脅領域一直小有名氣，似乎至少從 2022 年年中開始就活躍起來。雖然他們也採用惡劣的雙重勒索脅迫就範伎倆，但遠不如某些其他勒索軟體威脅者那樣明目張膽。但根據賽門鐵克長期持續觀察 Rever 的活動。一旦成功感染，被加密檔案將新增隨機的 8 個字元的副檔名。投放在受影響電腦上的贖金支付說明內容與 Babuk 投放的非常相似，並建議受害者透過即時加密通訊軟體 Tox Cha 與他們聯繫，但沒有說明贖金價格。

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.CryptLocker!g42
- SONAR.RansomPlay!gen1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Babuk
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/03/08

強勢回歸～Emotet殭屍網路，透過新一波垃圾郵件行動進行散播

Emotet 殭屍網路已在 3 月 7 日觀察到的新垃圾郵件行動中被散播。這是過去三個月中出現的第一個 Emotet 活動。該活動利用夾帶內含 .doc 檔案的 .zip 壓縮附件惡意垃圾郵件。.docs 附加大量的空字元，使每個檔案的大小膨脹到超過 500MB，而 .zip 附件本身的大小只有 600KB 左右。.doc 檔案嵌入混淆的 VBA 巨集，這些巨集從遠端網址下載 Emotet 的有效籌載。下載活動再次呼叫 .zip 壓縮提供大小膨脹的 Emotet .dll 二進位檔案。

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：

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：

- ISB.Downloader!gen433
- Scr.Malcode!gen22
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- W97M.Downloader
- WS.Malware.1

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。

2023/03/07

AresLoader～惡意軟體呼叫／引用軟體

AresLoader 是透過駭客論壇宣傳和銷售的惡意軟體呼叫／引用軟體。它於 2022 年 12 月左右首次出現，並且已經在真實網路環境發現它的幾個樣本。惡意軟體通常偽裝成合法的應用程式傳播給毫無戒心的用戶。一旦被感染，AresLoader 將連線到預先設定好的命令和控制 (C&C) 伺服器並下載預期的惡意軟體籌載。

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

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。

2023/03/07

ImBetter竊密程式～鎖定加密貨幣用戶

被稱為 ImBetter 全新的竊密惡意程式，已被用來針對加密貨幣用戶發動網路攻擊。該惡意軟體透過偽裝模仿知名和流行品牌的加密錢包 (例如：Metamask) 網站來進行傳播。ImBetter 具有竊取各種系統資訊和各種瀏覽器資料的功能，包括 cookie、登錄憑證、用戶設定檔和加密貨幣錢包。再將收集到的資料傳送到攻擊者預先設好的命令和控制 (C&C) 伺服器。

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
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/03/07

Sirattacker勒索軟體

Sirattacker 是一種源自 Chaos 勒索軟體家族的惡意軟體變種。最近在網際網路上發現這種勒索軟體的傳播行動。Sirattacker 執行檔偽裝成以太幣挖礦程式，傳播給毫無戒心的使用者。該惡意軟體將加密用戶的檔案，並在加密檔案中附加隨機式 4 個字元的副檔名。Sirattacker 會在命令提示字元中顯示勒索贖金支付說明，並將桌面背景替換為包含勒索贖金支付說明的圖片。

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：

- AGR.Terminate!g2
- SONAR.SuspDrop!gen1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Sorry
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

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

2023/03/07

CMLocker勒索軟體日益增加

在過去幾個月裡，一種名為 CMLocker 的勒索軟體一直在全球各地到處肆虐。如果不幸被其感染，被加密的檔案通常會被附加 .CMLOCKER 副檔名。與其他勒索軟體不同的是，CMLocker 背後攻擊者並沒有採用雙重勒索伎倆，似乎也不會在受害者的環境中橫向傳播。在受害者電腦留下的贖金說明中，他們要求價值 980 美元的比特幣。

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：

- AGR.Terminate!g2
- SONAR.Heur.Dropper
- SONAR.SuspBeh!gen93
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.6
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

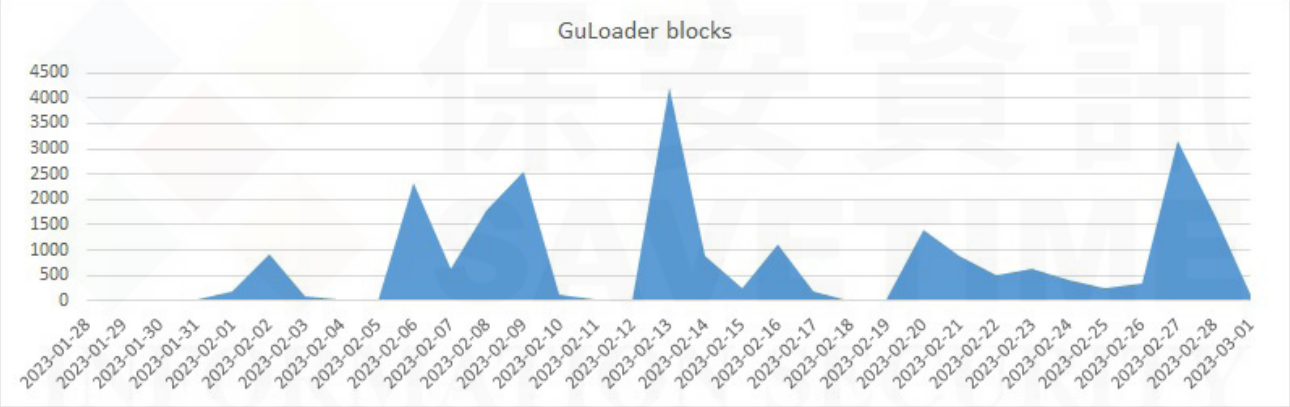
2023/03/06

防護亮點：第一時間成功攔截～GuLoader隱藏在眾目睽睽之下的先進惡意軟體下載程式

～防護亮點～

GuLoader 是一種進階型的 shellcode (利用軟體漏洞讓 CPU 執行特定程序的機械碼)，GuLoader 利用多種對抗分析的方式來增加反向工程的難度，使得它更難被偵測到。它的終極目標是傳遞一系列的惡意軟體，包含勒索軟體 (ransomware)、偷取敏感資訊的惡意軟體 (infostealers)、偷取金融資訊的惡意軟體 (banking Trojans)、遠端存取木馬 (RAT)、代理程式 (Proxy) 等。賽門鐵克威脅獵手團隊最近在一篇名為 "Bluebottle：發動攻擊非洲法語系國家銀行行動的駭客組織" (Bluebottle campaign targeting banks in French-speaking African countries) 的網誌中介紹了關於 GuLoader 的初階攻擊方式。

我們經常觀察到 GuLoader 是透過垃圾郵件的方式來散佈包含多種版本的 ISO 檔案，這些 ISO 檔中嵌入了 VBE 腳本，而 VBE 腳本再建立另一個 Powershell 腳本並執行它。



有多種 *GuLoader* 被偵測到，此處僅顯示 *Scr.Malcode!gen36*

雖然 GuLoader 不是什麼新的惡意軟體，但有趣的是作者為了不被偵測到而採取的措施。上面提到的 ISO/VBE 攻擊大致流程是……一開始一個經過代碼混淆的 Powershell 腳本去 Google Drive 下載並取出 GuLoader shellcode(使用 base64 編碼格式)，然後藉由 Windows API (CallWindowProcA) 將 shellcode 解碼 (base64)。從這裡開始 GuLoader 的作者就已進行避免偵測或延緩分析的措施。這些公告並不打算過於強調細節或技術性資訊，因此我們將儘量簡化說明。

GuLoader的反偵測技巧

- 反防毒軟體 #1：GuLoader 首先試圖防止作業系統從與 GuLoader 相關的 shellcode 區塊生成可執行檔，這是一個非常古老的技巧。
- 反除錯 #1：GuLoader 透過 Windows API 設置一個向量例外狀況處理常式(VEH)，並將代碼執行流指向到受管理的異常處理程序，該程序會嘗試捕捉由 EXCEPTION_SINGLE_STEP(TrapFlag) 引起的異常。 TrapFlag 允許處理器在單步模式下運行，可以操縱它以防止追踪。
- 反除錯 #2：反硬體間斷點和反軟體間斷點。硬體和軟體的間斷點是指在除錯時的暫停事件。GuLoader 會檢查這些事件並試圖防止它們。

- 反虛擬機 #1：記憶體分頁掃描。GuLoader 使用 NtQueryVirtualMemory API 掃描整個記憶體和處理程序，檢查是否有任何虛擬機 (VM) 或除錯工具相關的字串。
- 防禦逃避 #1：Heaven's Gate 是一種在 2000 年代中期為了相容性目的而使用的一種方法，允許在 32 位元程序中執行 64 位元程式碼。GuLoader shellcode 使用 Heaven's Gate 執行一個 64 位元程式碼中介(stub)使其不被注意。
- 反虛擬機 #2：GuLoader 檢查是否存在與 QEMU(VM) 模擬器相關的文件，例如：C:\Program Files\Qemu-ga\qemu-ga.exe 和 C:\Program Files\qga\qga.exe。
- 反除錯 #3：GuLoader 對 DbgBreakPoint 和 DbgUiRemoteBreakin 進行修補，來避免除錯器將其加入主機的執行程序當中。
- 防禦逃避 #2：移除 NTDLL32 中的 Hooks(用來插入自定義程式碼或函數)。GuLoader shellcode 掃描 NTDLL 中的 SYSCALL 狀態模式，提取 SYSCALL 編號並將函數代碼恢復到原始狀態。
- 反沙箱 #1：列舉視窗。GuLoader 呼叫 EnumWindows API 來計算在受害者機器上運行的上層視窗(無論可見與否)。如果數量低於 12，則 shellcode 終止。
- 反除錯 #4：ThreadHideFromDebugger。一種常見的反除錯技術，利用 NtSetInformationThread API 來有效的將執行緒標記為對除錯器不可見。
- 反沙箱 #2：GuLoader 使用各種 API 來列舉 Windows 驅動程式、已安裝的軟體和服務，並將它們的雜湊值與預先儲存的雜湊值進行比較。
- 反除錯 #5：ProcessDebugPort。Guloader 呼叫 NtQueryInformationProcess 來檢測是否有除錯器附加到它的處理程序中。

在多次嘗試隱藏之後，GuLoader shellcode 使用執行程序掏空技術 (Process Hollowing) 將自己注入到另一個執行程序當中，執行程序掏空技術是一種代碼注入技術，可以將記憶體中合法執行程序的可執行區段替換(或附加)為惡意代碼。

最後，在經過一連串的反偵測技巧 (在我們的案例中顯然是不成功的) 之後，GuLoader 將下載最終有效負載。在這個特定的案例中，有效負載是臭名昭張的 Agent Tesla。

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅的**零時差**攻擊，能通過以下方式識別 GuLoader：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen36

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)。

欲深入瞭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。

欲深入瞭解更多有關於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。

2023/03/06

吃閉門羹～賽門鐵克讓中國駭客組織Mustang Panda的新後門無用武之地

Mustang Panda (MQTTang) 是一個中國進階持續威脅 (APT) 駭客組織，自 2017 年以來一直活躍。該組織主要針對東南亞國家，專注於竊取政府機構、國防承包商和電信公司的機敏資訊。MQTTang 的攻擊技術包括社交工程、魚叉式網路釣魚電子郵件和惡意軟體攻擊。一個非現有公開可用惡意軟體的新自定義後門已被歸於該組織。該後門使用一個簡單的遠端 shell，但確實顯示 Mustang Panda 仍在積極使用和測試新技術。受害者尚未得到證實，但有類似於針對歐洲政治實體的網路攻擊行動。

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：

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

基於機器學習的防禦技術：

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

2023/03/05

偷雞不著蝕把米：電玩破解程式讓玩家因小失大

眾所周知，電玩破解程式、盜版軟體和破解軟體的偏愛者是網路犯罪份子最常鎖定的目標。在最近一個案例中，賽門鐵克觀察到有些生存射擊遊戲--堡壘之夜 (Fortnite) 的玩家在搜尋優勢時成了勒索軟體攻擊的目標。攻擊者將勒索軟體偽裝成“Fortnite Leecher and Slayer”，對受害者的檔案進行加密並新增一個隨機 4 個字元的副檔名。在受感染的機器上留下勒索說明檔，要求支付 30 元的波蘭茲羅提幣為贖金 (在撰寫本文時相當於 6.82 美元)。

在堡壘之夜 (Fortnite) 的情境下，leecher 是加入小隊或派對的人，目的是獲得獎勵和利益而不為團隊努力做出任何貢獻。換句話說，他們是團體中的寄生蟲意圖不勞而獲。另一方面，slayer 是積極參與並為團隊成功實現遊戲目標做出貢獻的角色。他們擔任領導角色，通常具有很強的溝通技巧和遊戲知識。

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

2023/03/05

使用破解軟體請小心～MacOS平台上又見Honkbox惡意挖礦程式

最近，Honkbox 惡意挖礦程式似乎再度發威，該惡意程式自 2019 年以來就在 MacOS 平台上經常造成災害。該威脅同時也是具有多個元件的惡意挖礦程式，據報導，至少有三個變種。攻擊者一直在 MacOS 用戶圈受歡迎的破解軟體中暗藏木馬來擴大散播。它主要影響消費者，但企業也無法倖免。

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：

- OSX.Trojan.Gen