保安資訊--本周(台灣時間2022/01/07)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 2.123 億次攻擊。這些攻擊中有 96% 在感染階段前就被有效阻止：**(2022/01/02)**

- 在**24萬4,100**台端點上，阻止了**1.204億**次嘗試掃描**Web**服務器的漏洞。
- 在**47萬6,200**台端點上，阻止了**3,800萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬900**台**Windows**伺服主機上，阻止了**2,860萬**次攻擊。
- 在**18萬6,300**端點上，阻止了**1,080萬**次嘗試掃描伺服器漏洞。
- 在**10萬6,100**台端點上，阻止了**510萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬2,500**台端點上，阻止了**390萬**次嘗試利用的應用程式漏洞。
- 在**39萬500**台端點上，阻止了**1,210萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,600**台端點上，阻止了**400萬**次加密貨幣挖礦攻擊。
- 在**4萬1,300**台端點上，阻止了**410萬**次向惡意軟體**C&C**連線的嘗試。
- 在**8,100**台端點上，阻止了**19萬1,900**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。

2022/01/06

以假日為主題的 Konni 遠端存取木馬 (RAT)

Konni 是一種遠端存取木馬 (RAT)，自 2014 年初就在真實環境中被觀察到。Konni 惡意軟體家族可能與 APT37 相關，是自 2012 年以來活躍的北韓網路間諜組織。

2021 年 12 月，該組織利用節日慶祝活動，對俄羅斯大使館外交官發動攻擊。發送所謂“恭賀新喜”的電子郵件，希望能吸引收件者，並附有惡意的 ZIP 壓縮檔。解壓縮附件檔後將顯示節日的螢幕保護程式。如果該誘導檔案被點擊，初始攻擊將會開始，連線到攻擊者 C&C 伺服器，然後 Konni RAT 下載作為其最終有效籌載。如果行動成功，攻擊者可完全控制受感染的系統。

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

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。

2022/01/05

新的 Zloader 木馬在真實環境中，利用微軟的簽名驗證

一項與 Zloader (一種專門設計來竊取用戶憑證的銀行惡意軟體) 有關的新行動，已在真實環境中被發現。該惡意軟體利用微軟的簽名驗證機制，將其有效籌載注入已簽名的系統 DLL 中，以隱藏其在受感染系統上的存在。一個名為 Atera 的合法遠端監控和管理軟體被用作該感染鏈的一部分，據報導 Conti 勒索軟體組織使用相同的軟體來獲得持久性和遠端存取。

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.MBT
- Trojan.Malfilter

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：

- Web Attack: Webpulse Bad Reputation Domain Request

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。

2022/01/04

假冒破解軟體下載，連向下載假冒的破解軟體導致資訊被竊

由於 Log4J 等漏洞幾乎每隔一天就會出現在新聞中，因此像社交工程這樣的惡意軟體傳遞機制經常被視而不見。社交工程仍然是向毫無戒心的用戶傳遞惡意軟體最有效方法之一。最近，我們觀察到利用“破解”軟體下載的幌子傳遞資訊竊取的惡意軟體。受害者被重新導向另一個網頁（透過諸如惡意廣告之類的方式），其中有破解版本的軟體可供下載。破解的版本實際上是一種竊取資訊的惡意軟體，在執行時會竊取重要的系統資訊，例如：瀏覽器 cookie、預設登錄、系統螢幕截圖等，並將其洩露回報給攻擊者。

賽門鐵克的網路防護技術入侵防禦系統 (IPS)，可以在瀏覽網頁階段就阻止感染，以防止進一步感染／損壞系統。

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：

- Packed.Generic.497
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

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 68
- Malicious Site: Malicious Domain Request 69
- Malicious Site: Malicious Domain Request 71
- System Infected: Infostealer Activity 16

2022/01/04

Purple Fox (*紫狐)，Rootkit感染

最近的惡意軟體行動被發現執行著使用 AutoIt 編譯並命名為“Telegram Desktop.exe”的惡意安裝程式。如果被觸發，將植入兩個檔案，一個是合法的 Telegram 安裝程式“Telegram.exe”和一個惡意下載程式“TextInputh.exe”。AutoIt 腳本會協助啟動 TextInputh.exe，攻擊的下一階段將開始。將建立與硬編碼 C&C 伺服器的連接以下載兩個附加檔案，其中一個是壓縮 (RAR)檔案。此壓縮檔包含最終有效籌載，其中包括 Purple Fox Rootkit。

如果成功部署，Purple Fox Rootkit 將停用使用者帳戶控制 (UAC)。UAC 是一項重要的安全功能，可幫助防止未經授權的存取並幫助減輕惡意軟體的影響。

保安補充：AutoIT 可以將人為操作 Windows 軟體的動作做成批次檔，這樣就可以用來自動操作 Windows 軟體。

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：

- Hacktool.Rootkit
- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan Horse
- 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。

2022/01/03

Aberebot 攻擊印度行動裝置使用者

早在 2021 年 11 月， 行動威脅版圖就出現 Aberebot 的新變種。這種 Android 銀行惡意軟體繼續被觀察到，並且最近被發現針對印度用戶。一名威脅行動者一直聲稱自己是 DHL，冀望引誘受害者安裝 Aberebot，它本身偽裝成 DHL 行動應用程式 (App)。雖然在印度受到關注，但報告也顯示在其他國家也觀察到該行動。

當 Aberebot 注意到用戶的活動與某些應用程式和網站的互動 (利用輔助功能服務) 時，它能夠透過覆蓋網路釣魚頁面來竊取多個銀行、社交媒體帳戶和加密貨幣服務的用戶憑證。它還能夠執行典型操作，例如：收集敏感裝置資訊、存儲的檔案、聯絡人和簡訊。

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：

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：

- AppRisk:Generisk

2022/01/02

自動化加密貨幣的行動

與加密貨幣相關的惡意活動仍然接二連三發生，並且沒有停止的跡象。威脅態勢由於受到企圖竊取加密錢包和劫持資源以營運加密貨幣的團體和個人的影響而陷入癱瘓。最近，至少從 2019 年以來一直威脅行動者曝光了。多年來，他們不斷發展攻擊鏈，最終目標是入侵主機並使用它們來挖礦，而受害者並不知情。

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

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。