保安資訊--本周(台灣時間2022/10/28)
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 99 萬 700 台受保護端點上總共阻止了 1.365億次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2022/10/24)**

- 在**18萬2,400**台端點上，阻止了**6,500**萬次嘗試掃描**Web**服務器的漏洞。
- 在**34萬6,600**台端點上，阻止了**2,560**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬7,200**台**Windows**伺服主機上，阻止了**1,890**萬次攻擊。
- 在**12萬3,500**端點上，阻止了**490**萬次嘗試掃描伺服器漏洞。
- 在**4萬1,700**台端點上，阻止了**200**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬900**台端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在**33萬9,500**台端點上，阻止了**760**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬6,900**台端點上，阻止了**400**萬次加密貨幣挖礦攻擊。
- 在**5萬3,800**台端點上，阻止了**510**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,700**台端點上，阻止了**21萬2,800**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。

2022/10/27

變本加厲～大規模Fodcha殭屍網路釋出最新版本

Fodcha 是一個大規模的分散式阻斷服務攻擊 (DDoS) 殭屍網路，最初發現於 2022 年 4 月。眾所周知，該惡意軟體是透過利用已揭露的漏洞以及透過對安全性較低的 Telnet／SSH 憑證進行暴力攻擊來散播。據報導，Fodcha 最新版本目前四處流通。攻擊者已經更新使用的通信協議，並開始利用額外的演算法進行通信加密。據瞭解，Fodcha 有能力可以針對各種架構，包括arm、mips、mpsl 和 x86 等。

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：

- Linux.Lightaidra
- Linux.Mirai
- Trojan.Gen.NPE
- 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。

2022/10/26

MaxOfferDeal惡意程式變種繼續糾纏干擾MacOS用戶

賽門鐵克持續在 MacOS 環境中觀察到 MaxOfferDeal (又名Genieo) 惡意程式的變種。一旦成功部署，MaxOfferDeal 將劫持受害者的網路瀏覽器，並在使用者瀏覽網頁時會彈跳出多個協力廠商廣告。它還會將用戶的搜巡重定向到非預期的網站。這些通常是透過假冒更新程式和廣告軟體安裝程式的瀏覽網頁時的順道下載 (drive-by-download) 攻擊方式來傳播。

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
- OSX.Trojan.Gen.2

2022/10/26

VMware的CVE-2022-22954漏洞仍在真實網路環境遭大量濫用

CVE-2022-22954 是 VMware 身分管理方案 Workspace ONE Access and Identity Manager 中的一個遠端程式碼執行 (RCE) 漏洞，該漏洞早在 2022 年 4 月就已被披露。根據最近的一份報告，這個漏洞依舊在真實網路環境成為被大量濫用目標。利用 CVE-2022-22954 攻擊正在鎖定 Linux 平臺來散佈各種有效籌載。在最近的攻擊行動中觀察到的有效籌載包括 Mirai 惡意軟體，RAR1ransom 勒索軟體和 GuardMiner--這是一個 XMRig 挖礦惡意程式。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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：

- Web Attack: VMware WorkSpace One RCE CVE-2022-22954

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。

2022/10/25

RomCom 遠端存取木馬(RAT)被用於攻擊烏克蘭的軍事目標

RomCom 遠端存取木馬 (RAT) 在最近針對烏克蘭軍事基礎設施的目標式攻擊中已被發揮得淋漓盡致。該惡意軟體被認為出自於 Tropical Scorpius，也稱為 UNC2596 的駭客組織。該惡意組織也曾在今年 8 月初對古巴發動勒索軟體攻擊行動。RomCom RAT 攻擊鏈也包含釣魚郵件，其中嵌入各種偽裝成協力廠商網站軟體更新或安裝程式的惡意軟體執行檔連結。

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

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。

2022/10/25

WarHawk--出自SideWinder進階持續威脅(APT)駭客組織之手的全新後門程式

WarHawk 是一個全新的後門惡意程式，被認為出自於 SideWinder 進階持續威脅 (APT) 的駭客組織。根據一份最新報告，該 APT 最近一次攻擊行動已經將 WarHawk 後門散播給巴基斯坦的使用者。SideWinder APT 一直在利用內含於 .ISO 檔和 .LNK 檔的 PDF 檔為誘餌來進行惡意軟體散播。據觀察，在已經被揭露的行動中發現，WarHawk 後門被用來下載和執行 Cobalt Strike 作為最終有效籌載。

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：

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.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。

2022/10/25

全新的竊密程式變種：Temp Stealer(*臨時偷竊者)

Temp Stealer 是地下論壇上宣傳的一個全新的通用型竊密程式變種。該惡意軟體能夠從被攻擊的端點竊取滲出各種資料，包括加密貨幣錢包、瀏覽器資料、系統資訊以及 Discord 或 Telegram 等應用程式的資料。根據最近的一份報告，Temp Stealer 通常被偽裝成破解版軟體或序號產生程式，但也可以作為其他各種軟體的捆綁安裝程式傳播。

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。

2022/10/24

SARA編譯工具，助長「鎖死手機螢幕」的勒索軟體氾濫

最近，Android (*安卓) 手機行動平台上鎖定使用者螢幕的勒索軟體大流行，主因是透過駭客論壇和惡意網站向不知情的使用者散播。這些鎖定程式都是使用 SARA 所建立的，SARA 是一個將現有的 Android(*安卓) 手機行動平台上的勒索軟體重新編譯成假冒的客製化行動應用程式 (APP) 的工具。這個工具最近上架在一個著名的軟體開發和版本控制的公眾平台上，這意味著它是可以被公眾取得的，也必定衍生更多的相關攻擊事件。攻擊者可透過鎖定手機螢幕向受害者索取贖金，以換取解鎖密碼。

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。

- AppRisk:Generisk
- AdLibrary:Generisk

2022/10/21

Apache修補Commons Text程式庫重大漏洞CVE-2022-42889(亦稱Text4Shell)

一個影響 Apache Commons Text 程式庫的重大 (Critical) 漏洞被發現。該漏洞被認定為 CVE-2022-42889 (又名 Text4Shell)，如果成功利用，可以在有漏洞的伺服器上執行遠端程式碼。該漏洞影響到 Apache Commons Text 1.5 至 1.9 版本。Apache 軟體基金會已經發佈該軟體的修補版本 (1.10.0)，建議使用者在有漏洞的軟體實例上套用該更新。

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：

- Web Attack: Apache Commons RCE CVE-2022-42889

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS(data Center Security) 內建的 Apache 安全政策能與進階強化的自訂沙箱協防為該漏洞提供默認的運行時保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2022/10/21

BlackByte勒索軟體營運商採用全新的Exbyte資料滲出工具

賽門鐵克威脅獵手 (Threat Hunter) 團隊發現，至少有一個 BlackByte 勒索軟體 (Ransom.Blackbyte) 營運商的協作分潤夥伴機構，已經開始在他們的攻擊行動中使用一種全新客製化資料滲出工具。Exbyte 滲出工具是用 Go語 言所撰寫，其功能在將被盜檔案上傳到 Mega.co.nz 雲端儲存服務商。BlackByte 是一個勒索軟體即服務的營運模式，由 Hecamede 網路犯罪集團所維運。

在我們的部落格文章中有更多資訊可供參考：Exbyte：BlackByte勒索軟體組織已部署新的外洩工具。

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：

- Infostealer.Exbyte
- ISB.Heuristic!gen71
- Ransom.Blackbyte
- Trojan Horse
- 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：

- Web Attack: Apache Commons RCE CVE-2022-42889

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已於第一時間收錄於不安全分類列表中。

2022/10/20

全新的Bisamware勒索軟體

另一個嶄露頭角的勒索軟體：Bisamware--最近危害不少真實網路世界的用戶。這種常見的網路威脅幕後的黑手一直在利用夾帶惡意文件的惡意郵件作為感染媒介。目前，他們並沒有試圖在組織內橫向移動以加密其他機器，而是專注在誘使受害者的機器。

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：

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：

- Exp.CVE-2021-40444!g4
- Trojan.Gen.2
- Trojan Horse
- W97M.Downloader