保安資訊--本周(台灣時間2022/05/27)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1.966億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/05/22)**

- 在**22萬2,900**台端點上，阻止了**9,920萬**次嘗試掃描**Web**服務器的漏洞。
- 在**45萬4,300**台端點上，阻止了**3,690萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬1,000**台**Windows**伺服主機上，阻止了**2,200萬**次攻擊。
- 在**16萬6,700**端點上，阻止了**960萬**次嘗試掃描伺服器漏洞。
- 在**8萬2,700**台端點上，阻止了**410萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬2,400**台端點上，阻止了**410萬**次嘗試利用的應用程式漏洞。
- 在**35萬9,700**台端點上，阻止了**930萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,060**台端點上，阻止了**380萬**次加密貨幣挖礦攻擊。
- 在**11萬6,000**台端點上，阻止了**530萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,800**台端點上，阻止了**22萬2,500**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。

2022/05/26

Pymafka 供應鏈攻擊

最近的一次攻擊利用了一個惡意的 Python 套件（名為 "pymafka"），該套件已被上傳到一個熱門的 Python 套件索引（Python Package Index，簡稱 PyPI）套件庫，Pykafka 是一個已知的 Python 的 Kafka 用戶端。攻擊者透過使用與合法套裝軟體非常相似的名稱，意圖誘騙受害者下載惡意套裝軟體。Pymafka 被發現下載 Cobalt Strike 信標，它可能被用於攻擊的後期階段。活動期間，包括 Windows、Linux 和 macOS 在內的各種平臺都是攻擊目標，因為 pymafka 套件內的 Python 腳本會在植入作業系統特定的二進位檔案之前嘗試偵測受害者的平臺。

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：

- Meterpreter
- OSX.Trojan.Gen
- 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。

2022/05/26

ChromeLoader 瀏覽器劫持惡意軟體，鎖定 Windows 和 macOS 用戶發動傳播行動

ChromeLoader（也被稱為 Choziosi loader）是一種瀏覽器劫持惡意軟體，它改變瀏覽器的設定與配置，目的是將使用者流量轉到廣告網站。最近，利用這種惡意軟體的大多數行動都是針對 MacOS 和 Windows 用戶，為 Chrome 或 Safari 瀏覽器提供惡意的瀏覽器外掛。根據最新的報告，這種惡意軟體是以惡意 ISO 檔的形式散佈，偽裝成軟體或遊戲破解版，或透過社交媒體上的帖文誘餌，其中包含誘導下載惡意網址的連結或 QR Code。該惡意軟體的 macOS 變種是以 DMG 格式的檔案，包含 ChromeLoader 有效籌載的安裝程式腳本。

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
- 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。

2022/05/25

Ermac 2.0 已經在網路上大量流竄

Ermac 是一個 Android (*安卓) 網路銀行惡意軟體，至少從 2021 年中就已經存在。最近有報告指出，2.0版本主要透過熱門服務的假冒網站，但也會透過假冒的的瀏覽器更新網站散佈。這種惡意軟體正在地下論壇上出售（或以每月5000美元的價格出租），並有能力使用惡名昭彰和熱門的堆疊覆蓋 (overlay) 技術瞄準 400 多個銀行應用程式 (APP)。這種技術在銀行應用程式上顯示一個假冒的畫面，以誘騙使用者輸入他們的銀行帳密。

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

2022/05/25

Cobalt-Strike 信標透過假的概念證明 (POC) 程式碼散佈

根據最新的報告，一個未知的威脅者在 GitHub 上發佈兩個概念證明 (POC)，用於最近修補的 Windows CVE-2022-24500 和 CVE-2022-26809 漏洞的利用。後來發現，這些假的 POC 實際上是用 Cobalt Strike 感染設備。Cobalt Strike 是一個測試工具，通常被各種威脅者用來執行惡意命令或下載額外的有效籌載……等惡意行為。

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

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。

2022/05/25

GoodWill (*好心腸) 勒索軟體

勒索軟體通常是破壞性的，處理起來也很棘手，因為它只對攻擊者有利。然而，去年 3 月發現一個新的勒索軟體變種，它似乎走的是道德的路線，被稱為 GoodWill。GoodWill 目的是透過強迫他們的受害者做三件好事來向那些弱勢族群傳播善意。

- 善舉1：捐贈新衣服給無家可歸的人，記錄下這些善行，並在社交媒體上發佈。
- 善舉2：帶五個弱勢孩子去達美樂、必勝客或肯德基吃東西，拍照並錄影，然後發佈在社交媒體上。
- 善舉3：在附近的醫院為任何需要緊急醫療但無力支付的人提供經濟援助，錄製音訊並與營運商分享。

一旦完成這三項善舉並通過威脅者在社交媒體平臺的驗證，完整的解密工具包將與受害者分享。受感染的被加密檔將會以 .gdwill 作為其新的附檔名。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/05/23

Vidar 竊密程式透過惡意的 ISO 檔散佈

最近發現的一個攻擊行動，使用惡意的 ISO 檔來散佈 Vitar 竊密程式。威脅者一直在利用幾個偽裝成下載 Windows 11 作業系統的入口網站來散佈惡意軟體。這個最新的 Vidar 變種從攻擊者控制的 Telegram 和 Mastodon 社交媒體管道取得 C&C 通信細節。據報導，另一個類似的攻擊行動是利用被植入後門程式的 Adobe Photoshop Creative Cloud 應用程式的版本來散佈 Vidar。

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

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: 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。

2022/05/23

Twisted Panda 進階持續威脅 (APT) 組織 ，利用 Spinner 後門

根據最近一份報告，被稱為 Twisted Panda 的進階持續威脅 (APT) 組織的一系列新活動已被發現在網路上流竄。觀察到的活動被認為是長期針對俄羅斯有組織的間諜行動延續。該 APT 組織一直在利用一系列的工具和各種惡意軟體變種。其中有一個被稱為 Spinner 新後門，它同時具備能列舉 (搜尋和發掘) 遭入侵電腦的詳細資訊基本功能，以及在目標系統上執行額外有效籌載的能力。

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

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已於第一時間收錄於不安全分類列表中。

2022/05/22

Snake 鍵盤側錄程式透過惡意的 PDF 檔散佈

在惡意郵件行動中，Office 文件檔（如：DOCX 和 XLS 檔）是威脅者用來傳遞有效籌載的常見手段，而利用 PDF 不同的檔案格式聽起來可能不尋常，這使得欺騙用戶執行惡意檔案得逞機會大大提高。攻擊者常常採用與惡意 PDF 檔相關的幾個技巧包括嵌入檔、載入遠端代管的漏洞攻擊工具和加密的 Shellcode 等方式。這些戰術使攻擊能夠躲過安全軟體的檢查，最後的有效籌載“Snake鍵盤側錄程式”將被隱蔽地散佈。Snake 鍵盤側錄程式是一種竊取資訊的惡意軟體。

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：

基於行為偵測技術(Snoar)的防護：

- Heur.AdvML.B

檔案型(基於回應式樣本的病毒定義檔)防護：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Exp.CVE-2017-11882!g3
- Scr.Malcode!gdn30
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

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。

2022/05/20

針對 Linux 設備的惡意軟體：XorDDoS

這種惡意軟體被稱為 XorDDoS。它的名字來自於它與 C&C 伺服器通信時使用 XOR 為基礎的加密技術，以及它在分散式阻斷服務 (DDoS) 攻擊中的應用。這種惡意軟體針對 Linux 終端，特別是物聯網（IoT）設備和雲端基礎設施，以隱蔽的方式進行感染和操作。在過去的幾個月裡，由這種惡意軟體建立的僵屍網路有所增加，DDoS 攻擊也歸因於它們。

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.Xorddos
- Trojan Horse
- WS.Malware.1
- WS.Malware.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已於第一時間收錄於不安全分類列表中。

2022/05/20

Redis 伺服器被利用來植入 Kaiten 後門

Redis 是一個開放原始碼的資料結構儲存，用作資料庫、快取和訊息中介。CVE-2022-0543 是一個存在於某些 Redis Debian 套裝軟體的漏洞。該漏洞允許遠端攻擊者在 Redis 伺服器上執行任意程式碼。賽門鐵克的網路保護技術--入侵防禦系統 (IPS) 根據僵屍網路流量監測發現掃描結果，顯示該漏洞被用來在被攻擊的 Redis 伺服器上部署 Kaiten 後門。Kaiten 是一個用於發動 DDoS 攻擊的木馬。除了發動 DDoS 攻擊，它還可能停用程序、下載和執行其他任意檔案，或針對被攻擊設備發動 IP 位址偽裝攻擊。

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.Kaiten

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: Redis CVE-2022-0543

基於安全強化政策(適用於使用DCS)：

Data Center Security (DCS) Unix Prevention 政策提供 Redis 應用伺服器的防護。為 redis 伺服器新增 DCS Application 規則 (program path=/usr/bin/redis-server) 以強化 Default Daemon 沙箱的應用程式。