保安資訊--本周(台灣時間2022/08/26)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 96 萬 3,500 個受保護端點上總共阻止了1.501億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/08/22)**

- 在**19萬9,500**台端點上，阻止了**7,470**萬次嘗試掃描**Web**服務器的漏洞。
- 在**35萬3,900**台端點上，阻止了**2,660**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬9,500**台**Windows**伺服主機上，阻止了**1,800**萬次攻擊。
- 在**13萬1,600**端點上，阻止了**660**萬次嘗試掃描伺服器漏洞。
- 在**6萬1,100**台端點上，阻止了**290**萬次嘗試掃描在**CMS**漏洞。
- 在**11萬4,600**台端點上，阻止了**310**萬次嘗試利用的應用程式漏洞。
- 在**30萬8,400**台端點上，阻止了**700**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**670**台端點上，阻止了**350**萬次加密貨幣挖礦攻擊。
- 在**4萬7,600**台端點上，阻止了**510**萬次向惡意軟體**C&C**連線的嘗試。
- 在**6,000**台端點上，阻止了**17萬7,800**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。

2022/08/25

XWorm--具隱藏桌面的惡意 VPN 連線 (HVNC)攻 擊能力的遠端存取木馬(RAT)

XWorm 是一個遠端存取木馬（RAT），目前在地下論壇上出售。這種基於 .NET 的惡意軟體具有許多功能，目的是對受入侵的機器進行遠端控制、命令執行和資料收集運出。XWorm二進位檔案還可以植入額外的惡意有效籌載，並包含允許其執行隱藏桌面的惡意 VPN 連線（HVNC：Hidden Virtual Network Computing）--這是利用 VPN 預先已設定好的信任條件，透過入侵內網電腦而接手 VPN 授予的存取權限攻擊。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen23
- SONAR.SuspBeh!gen93
- SONAR.SuspDataRun
- SONAR.TCP!gen6
- SONAR.UACBypass!gen30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Dropper!g6
- Trojan.Gen.2
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/08/24

利用瀏覽網頁時順道下載 (drive-by-download) 所發動的 ArrowRAT 攻擊行動

ArrowRAT是一個遠端存取木馬 (RAT)，至少從 2021 年起就開始積極銷售。在過去的幾個月裡，賽門鐵克看到越來越多的活動，其中包括測試和順道下載 (drive-by-download) 攻擊行動。在這些攻擊行動中，威脅者試圖透過將惡意二進位檔案偽裝成遊戲駭客、軟體安裝程式（如Visual Studio）和更新修正（如谷歌更新）來引誘受害者。ArrowRAT 的功能並不是什麼新的或不常見，它是一個相當普通的遠端存取木馬。從熱門程度來看，不如 Remcos 等更有名的 RATs 那麼受歡迎。

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：

- HTrojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/08/24

針對南亞電信部門的 PivNoxy 和 Chinoxy 惡意軟體

根據最近一份報告，一個針對南亞電信公司的惡意行動一直在散佈 Chinoxy 和 PivNoxy 惡意軟體的新變種。攻擊者在攻擊初始階段一直利用夾帶 .doc 附件的魚叉式釣魚郵件。惡意檔案是利用一個被稱為 Royal Road 的漏洞探刺攻擊套件所建立。該攻擊利用 2017 年和 2018 年的微軟 Office 記憶體損毀 (Memory corruption) 漏洞。一旦植入程式存在遭入侵的機器上，大多會衍生更多有效籌載，進而獲得更深入的入侵與嚴重破壞，在某些回報案例中，Poison Ivy 遠端存取木馬已被證實為其中之一。

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：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Trojan Horse
- Trojan.Gen
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Mdropper
- Trojan.Shannel
- WS.Malware.1
- WS.Malware.2

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。

2022/08/23

利用 Zimbra 郵件協作系統的遠端程式碼執行漏洞 (CVE-2022-27925) 的攻擊，大幅增加

最近，觀察到威脅者利用 Zimbra 的多個漏洞--這是一個雲端代管的郵件協作軟體套裝，包括一個電子郵件伺服器和一個 Web 用戶端。在這份保護公告中，我們將介紹 CVE-2022-27925

，這是一個遠端程式碼執行漏洞，允許攻擊者上傳精心製作的壓縮檔，來進行目錄遍歷攻擊(directory traversal：一種利用網站的安全驗證缺陷或用戶請求驗證缺陷，來列出伺服器目錄的漏洞利用方式)。在攻擊中，Webshells 隨後被植入到目標位置，作為後門存取被攻擊的伺服器。

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：

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: Malicious ZIP File Upload

基於安全強化政策(適用於使用DCS)：

Symantec 的 DCS 內建伺服器安全政策即能阻止 Webshells 的植入。

2022/08/23

macOS 平台大量出現 XCSSET 惡意軟體，已危害大眾

最近在真實網路環境發現 macOS 平台獨有的 XCSSET 惡意軟體的新變種。最近散佈這種惡意軟體的行動中，威脅者一直在假的 Notes.app 應用程式中隱藏惡意的可執行檔。該惡意軟體利用多個 run-only 屬性的 AppleScript 程序檔，針對各種聊天應用程式和網路瀏覽器進行資訊竊取。在這個新的 XCSSET 變種中，作者還為 python3 更新了更能充分利用 python 功能的腳本，以適應最新的 macOS Monterey 版本。

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
- Trojan Horse
- 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。

2022/08/23

Redeemer (*救贖者)--勒索軟體

Redeemer 是一個透過附屬程式在網路犯罪論壇上傳播的勒索軟體變種。上個月這個勒索軟體家族的一個新的 2.0 版本在網上被宣傳。根據作者的說法，它帶有新的附屬 GUI 工具包，對 Windows 11 有更好的支援性，修改勒索說明/贖金支付說明和其他一些改進。Redeemer 勒索軟體包括清除事件日誌和刪除受感染機器上的任何陰影複製 (shadow copies) 或系統備份的功能。被加密的檔案會新增 .redeem 的副檔名。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspBeh!gen57
- SONAR.SuspDrop!gen1
- SONAR.SuspLaunch!g18
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

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

2022/08/22

Lumma 竊密程式，已在真實網路環境傳出災情

在多如過江之鯽的網路生態黑社會，能嶄露頭角的惡意程式，一定有相當的能耐，最近 Lumma 竊密程式就是一個例子。Lumma 竊密程式是橫空出世的殺手級產品，它的功能與作用和其他許多竊密程式大同小異，都能配合當前環境而調整其功能及作用。Lumma 主要功能如下：

- 竊取多個瀏覽器的登錄憑證、cookies和自動填表資訊
- 在文字檔中存儲不同類型的資訊
- 從與加密貨幣錢包有關的瀏覽器外掛中竊取資料
- 針對與雙因子和多因子認證（2FA/MFA）和密碼管理有關的其他基於 Chrome 瀏覽器外掛程式
- 透過檢查 AppData 中預設錢包檔案位置，竊取與加密貨幣錢包應用程式有關的錢包和機密文件

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
- Packed.Vmpbad!gen38
- Trojan.Gen.2

2022/08/22

偽裝成 Zoom 安裝程式：PNetwire 惡意程式

Netwire 是一個已經存在幾年的遠端存取木馬，現在仍然經常被全球的駭客組織和個人所採用。目前 Netwire 惡意活動仍是主要透過惡意郵件和瀏覽網頁時的順道下載 (drive-by-download) 來發動。多年來，我們已經看到各種社交工程伎倆被用來引誘受害者，從普通的報價、付款和各

項交易，到熱門的新聞和時髦的流行。最近，賽門鐵克觀察到一個威脅者試圖把他的 Netwire 二進位檔案偽裝成 Zoom 安裝程式來散佈。眾所周知，Zoom 是一個主要的視訊會議服務，其用戶在 COVID-19 疫情爆發期間大幅增加。

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.Netweird

2022/08/22

BianLian -- 由 GoLang 編譯語言撰寫勒索軟體

BianLian 是一個用 Go(GoLang) 程式設計語言編寫的新型勒索軟體變種。據報導，BianLian 在上個月剛被發現，它的目標是跨產業別的的多個組織。該惡意軟體對使用者檔案進行加密，並將 .bianlian 副檔名附加到這些加密檔案上。一旦加密完成，該勒索軟體就會投放勒索 (支付贖金) 說明，並從被攻擊的機器上刪除自己。這個勒索軟體變種背後的威脅者採用雙重敲詐勒索戰略，脅迫受害者如不付贖金就會公開洩露被竊取的機密資料。

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：

- AGR.Terminate!g2
- SONAR.Cryptlocker!g80
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- WS.Malware.1

2022/08/22

惡意軟體 Grandoreiro，針對西班牙語國家的組織

在真實網路環境觀察到一個全新的正在進行涉入 Grandoreiro 銀行木馬並針對西班牙語國家的大規模攻擊行動。威脅者利用偽裝成政府官員信件的魚叉式網路釣魚郵件，引誘收件人下載惡意軟體二進位檔案。Grandoreiro 使用一種被稱為二進位填充 (binary padding) 的技術，將多個 .bmp 點陣圖添加到二進位檔案中，以擴大它的大小 (超過400MB)，從而試圖逃避沙箱偵測。該惡意軟體的目標是受害者的銀行資訊，但也有額外的後門功能，允許它執行任意命令……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：

基於行為偵測技術(Snoar)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

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：

- System Infected: Trojan.Backdoor Activity 568

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。

2022/08/21

Apple Pay--蘋果行動支付易遭受簡訊釣魚詐騙，造成用戶衝擊

在過去的一年裡，透過簡訊（SMS）進行的網路釣魚活動穩定成長--這些攻擊在網路安全領域也被稱為 "smishing*簡訊釣魚"。這些行動大多導致受害者被引誘到虛假網站輸入他們的憑證，但也有一些情況是這些網站會誘導他們安裝行動惡意軟體。說到憑證式網路釣魚，威脅者主要藉故自己是與金融有關的服務商，如銀行。最近有一個針對蘋果用戶的詐騙行動，受害者會收到一則簡訊，通知他們的蘋果支付已被暫時中止，要求他們登入一個網站以確認細節。如果成功被騙，假網站就會試圖盜取使用者的金融資訊。

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：

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。

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。