保安資訊--本周(台灣時間2022/07/08)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 100 萬個受保護端點上總共阻止了1.782億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/06/27)**

- 在**20萬6,700**台端點上，阻止了**8,700**萬次嘗試掃描**Web**服務器的漏洞。
- 在**39萬800**台端點上，阻止了**3,420**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬7,900**台**Windows**伺服主機上，阻止了**2,040**萬次攻擊。
- 在**14萬300**端點上，阻止了**840**萬次嘗試掃描伺服器漏洞。
- 在**7萬300**台端點上，阻止了**350**萬次嘗試掃描在**CMS**漏洞。
- 在**10萬6,500**台端點上，阻止了**320**萬次嘗試利用的應用程式漏洞。
- 在**30萬5,500**台端點上，阻止了**810**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2萬5,700**台端點上，阻止了**490**萬次加密貨幣挖礦攻擊。
- 在**10萬1,200**台端點上，阻止了**670**萬次向惡意軟體**C&C**連線的嘗試。
- 在**6,300**台端點上，阻止了**39萬1,400**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。

2022/07/07

Maui 勒索軟體被用於發動醫療行業的目標式攻擊

賽門鐵克安全機制應變中心團隊瞭解到最近美國國土安全部網路安全暨基礎設施安全局 (CISA) 和聯邦調查局 (FBI) 觀察到一些針對 Maui 勒索軟體活動的警報。據報導，至少從 2021 年 5 月開始，這種惡意軟體就已經鎖定醫療和公共衛生 (HPH) 部門為主要攻擊目標。據信，Maui 勒索軟體被設計由威脅者在透過命令列介面與惡意軟體二進位檔案互動下手動執行。一旦目標使用者資料被攻擊者識別，該惡意軟體就會使用 AES 128 位元加密技術對檔案進行加密。

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：

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.C

2022/07/06

趁火打劫：Rozena 後門程式利用Follina漏洞

威脅者繼續將最近微軟 Windows 支援診斷工具的遠端程式碼執行 (RCE) 漏洞 (CVE-2022-30190，又名 Follina 漏洞) 納入到他們的攻擊鏈中。最近，人們觀察到一個被稱為 Rozena 的後門幕後黑手透過惡意郵件利用這個漏洞乘虛而入。

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
- Trojan.Gen.NPE
- Trojan.Malscript

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: MSDT Remote Code Execution CVE-2022-30190

基於安全強化政策(適用於使用DCS)：

DCS預設策略強化了MS Office應用程式。DCS防止MS Office應用程式啟動命令直譯器，包括cmd.exe、powerhell.exe和其他子程序。此外，對於這個CVE編號的漏洞，可以透過將*\msdt.exe新增到沙箱執行控制 "Microsoft Office不可執行的程式 "中來防止RCE漏洞。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2022/07/06

Raspberry Robin (*樹莓羅賓) 蠕蟲透過 USB 裝置傳播

Raspberry Robin (也被稱為 "QNAP蠕蟲") 是一種具有蠕蟲性質的惡意軟體，最初在 2021 年 9 月被發現。據瞭解，該惡意軟體藉由惡意 .lnk (捷徑) 檔掩護透過受感染的 USB 隨身碟傳播。感染過程包含下載和執行含有惡意程式庫的 .msi 安裝包。Raspberry Robin 還利用微軟標準安裝程式 (Microsoft Standard Installer:msiexec.exe) 的程序連接到攻擊者預先配置的 C2 伺服器。在某些情況下，也會利用命令和控制 (C&C) 基礎設施協同惡意軟體與 TOR 網路節點的連接。

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：

- CL.Downloader!gen20
- Downloader
- Packed.Generic.553
- Trojan Horse
- 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
- Heur.AdvML.C

基於安全強化政策(適用於使用DCS)：

DCS 內建 Windows 的強化功能，能提供針對 Rasberry Robin 威脅的零時差攻擊保護。DCS 初始配置就有鎖定防止任意下載 .msi 安裝包和啟動 msiexec.exe 連接到外部 C&C 基礎設施的預防功能。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2022/07/05

VSingle 惡意軟體釋出升級版的變種

VSingle 是由 Lazarus 威脅集團使用一種 HTTP 機器人惡意軟體。VSingle 具有從攻擊者那裡接收執行指令以及下載和執行額外外掛程式的功能。最新的 VSingle 變種已經更新，它現在可以從攻擊者控制的 Github 資料庫中檢索 C&C 伺服器的通信資訊。除了 Windows 變種外，VSingle 也針對 Linux 作業系統平臺。

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：

- 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: 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。

2022/07/05

新的 Xloader 威脅行動利用隱寫術

Xloader 是惡名昭彰的 Formbook 竊密程式改名換姓後的變種。與它的前身一樣，Xloader 目的是竊取憑證和網路瀏覽器 cookies、鍵盤、按鍵側錄，以及截圖和竊取其他各種使用者的資料。在一個新的威脅行動已發現其初始階段利用夾帶 .pdf 附件的垃圾電子郵件。並使用 .xlsx 和 .rtf 格式嵌入其他惡意檔案，來增加整個感染鏈的複雜度。這個 Xloader 傳播行動還利用隱寫技術，將惡意內容隱藏在點陣圖檔中。

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：

- Packed.Generic.661
- Scr.Malcode!gdn30
- Trojan Horse
- Trojan.Formbook
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Mdropper

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。

2022/07/04

Chropex 劫持 MacOS 使用者的瀏覽器

最近在 macOS 的威脅中又觀察到另一個瀏覽器劫持程式。雖然 Chropex 主要活躍在美國，但賽門鐵克繼續在其他國家觀察到更多實例。這個劫持程式背後的威脅者，一直在透過惡意廣告行動和順道下載來散佈，在 macOS 的威脅環境中也是很典型的感染媒介。如果它成功地劫持受害者的瀏覽器，它將打開 Safari 瀏覽器並顯示網頁廣告，但也監視 Safari 瀏覽器的搜尋，以便注入更多的廣告。

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.Chropex

基於行為偵測技術(Snoar)的防護：

- SONAR.Chropex!g1

2022/07/04

MedusaLocker 勒索軟體利用 RDP 漏洞獲取網路存取權限

賽門鐵克安全機制應變中心團隊瞭解到最近 CISA 和 FBI 觀察到 MedusaLocker 勒索軟體的一些活動所發佈之警報。此惡意軟體是在 2019 年底首次發現。根據發佈報告，最近在 2022 年 5 月觀察到這種勒索軟體變種的最新活動。MedusaLocker 是一種勒索軟體即服務 (RaaS) 的惡意軟體，已知它利用遠端桌面協定 (RDP) 的漏洞來存取目標網路。MedusaLocker 整合刪除備份和復原選項的功能，並具有透過 Internet Control Message Protocol (ICMP)--網際網路控制訊息協定來掃描並發現該系統的網路連線狀態。

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.SuspBeh!gen54
- SONAR.SuspDrop!gen7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Cryptolocker

- Ransom.Locky!g35
- Ransom.MedusaLocker
- 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：

- Attack: Ransom.Gen Activity 56

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。

2022/07/03

Bahamut (*巴哈姆特) 的安卓間諜軟體被偽裝成經加密保護的訊息應用 APP

被稱為 Bahamut 的 APT 組織至少從 2017 年開始就在中東和南亞地區開展網路間諜行動。他們使用經客製化的惡意軟體和工具，其中包括一個安卓惡意軟體。最近，他們的一個行動被曝光，他們試圖透過釣魚網站引誘受害者，企圖用他們的安卓間諜軟體的一個變種來感染他們，該間諜軟體偽裝成一個提供經加密保護的訊息應用 APP。

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。

- AdLibrary:Generisk
- AppRisk:Generisk

2022/07/01

SolidBit，一支模仿 LockBit 的勒索軟體

SolidBit 初期是 Yashma (又名 Chaos) 勒索軟體的變種，儘管後者的版本已經在地下論壇上被洩露，但 SolidBit 並沒有原封不動地使用遭洩露的程式碼。SolidBit 包括一些新增或變更的內容，其中之一是支持聊天功能，這可能是他們從 LockBit 獲得的東西，因為聊天介面與 LockBit 非常相似。

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

基於行為偵測技術(Snoar)的防護：

- SONAR.Cryptlck!g114

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C

2022/07/01

8220 威脅集團針對 Linux 的持續行動

一個針對 Linux 平臺火熱的威脅活動，與一個被稱為 8220 的威脅集團有關，已看到發佈pwnRig 加密惡意軟體的更新版本和 IRC 機器人。攻擊者利用 CVE-2022-26134 (Atlassian Confluence) 和 CVE-2019-2725 (Oracle WebLogic) 遠端程式碼執行 (RCE) 漏洞進行初始存取。在利用上述漏洞後，一個載入程式被部署，進而將有效籌載下載到被入侵的系統中。

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.Backdoor.Kaiten
- Linux.Kaiten
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Malware.2

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: Oracle Weblogic RCE CVE-2019-2725
- Web Attack: Atlassian OGNL Injection CVE-2022-26134

基於安全強化政策(適用於使用DCS)：

擁有 Confluence 伺服器實例的 DCS 客戶可使用預設強化規則進行保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2022/07/01

PennyWise 明目張膽從 YouTube 引誘受害者

在威脅領域中又發現另一個竊密程式。這個被稱為 PennyWise 的軟體具有常見的資訊竊取能力，這意味著它可以竊取瀏覽器和加密貨幣相關的應用程式資料。在最近一次行動中，威脅者利用 YouTube 來散佈惡意軟體，用 YouTube影片 (例如：關於加密貨幣挖礦) 引誘受害者，在影片旁白中提供下載連結，最終導致受害者感染 PennyWise 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/06/30

YTStealer 竊密程式對 YouTubers 的認證 cookies 及相關資訊虎視眈眈

多年來，YouTube的受歡迎程度一直屹立不搖--該平臺匯集大量的內容創作者，許多人每天都有數百萬的觀眾。如果著名的 YouTube 內容創作者和有影響力的人帳戶被洩露，那會怎樣？它可能為讓此被入侵帳戶的擁有者和他們的觀眾開啟夢魘的序曲。目前，除了常見的憑證釣魚，尚未有很多惡意軟體鎖定該平臺。但最近有報導稱，一個被稱為 YTStealer 的竊密程式專門試圖劫取 YouTube 用戶的認證 cookies，並竊取受害者帳戶／頻道的各種資訊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan.Gen.9

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
- System Infected: Trojan.Backdoor Activity 564