保安資訊--本周(台灣時間2022/03/11)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 130 萬個受保護端點上總共阻止了 2.0463 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/03/06)**

- 在**24萬6,900**台端點上，阻止了**1.066億**次嘗試掃描**Web**服務器的漏洞。
- 在**50萬4,600**台端點上，阻止了**4,320萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**9萬1,000**台**Windows**伺服主機上，阻止了**2,640萬**次攻擊。
- 在**19萬5,300**端點上，阻止了**1,040萬**次嘗試掃描伺服器漏洞。
- 在**10萬300**台端點上，阻止了**510萬**次嘗試掃描在**CMS**漏洞。
- 在**15萬3,700**台端點上，阻止了**410萬**次嘗試利用的應用程式漏洞。
- 在**43萬400**台端點上，阻止了**1,290萬**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**470萬**次加密貨幣挖礦攻擊。
- 在**13萬5,300**台端點上，阻止了**580萬**次向惡意軟體**C&C**連線的嘗試。
- 在**6,900**台端點上，阻止了**26萬6,700**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。

2022/03/10

在Linux核心版本發現提權漏洞："Dirty Pipe (*髒管)"

3月7日，一名安全研究人員披露 Linux 核心版本中的一個漏洞，該漏洞可允許提權 (權限提升)。該漏洞被公開命名為 Dirty Pipe，並被納入通用漏洞揭露計畫 (Common Vulnerabilities and Exposures, CVE®)編號 CVE-2022-0847，該漏洞允許未經授權使用者覆寫唯讀檔案中的資料。受影響的核心版本從 5.8 開始，而在 Linux 5.16.11、5.15.25 和 5.10.102 之後，它已經被修復。

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：

- Exp.CVE-2022-0847

2022/03/10

Nokoyawa 勒索軟體顯示出與 Hive 的相似之處

一個被稱為 Nokoyawa 的新勒索軟體變種已經在真實環境大量爆發。據報導，Nokoyawa 與 Hive 勒索軟體變種有一定程度的相似之處。與 Hive 類似，Nokoyawa 在攻擊的初始階段利用 Cobalt Strike以及額外的工具，如：GMER，用於後期的防禦規避。Nokoyawa 目前似乎以南美洲的受害者為目標，主要在阿根廷。

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：

- Backdoor.SystemBC
- Ransom.Gen
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於行為偵測技術(Snoar)的防護：

- SONAR.Ransomware!g1
- SONAR.Ransomware!g7

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/03/09

可惡的惡意垃圾郵件行動，向烏克蘭人民落井下石散播 FormBook 惡意軟體

Formbook 是一支竊密程式，最近在一個針對烏克蘭人民的惡意郵件行動中被觀察到。該電子郵件包含一個惡意的微軟 Excel 附件，據稱是假冒一份從政府獲得資金的批准信。如果該檔案被執行，CVE-2017-11882 的漏洞將入侵電腦，隨後從遠端伺服器下載 Formbook 有效酬載。

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：

- Exp.CVE-2017-11882!g5
- Trojan.Formbook
- Trojan Horse
- Trojan.Gen.MBT
- 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已於第一時間收錄於不安全分類列表中。

2022/03/09

微軟 3 月補丁發佈的覆蓋範圍詳細資訊

微軟 3 月 8 日發佈定期排定的每月更新。對於 3 月份的發佈，微軟已經解決 71 個漏洞。

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：

- Exp.CVE-2022-21990

2022/03/09

觀察到稅務發票垃圾郵件會傳遞 Remcos RAT

據觀察，Remcos RAT 在最近垃圾郵件攻擊中被傳遞。這些訊息很短並假冒與稅務相關的發票，以誘使收件者打開附件的壓縮檔。壓縮檔內的可執行檔會嘗試繞過 UAC 並控制使用者的系統。

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：

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：

- 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

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。

2022/03/09

JSSLoader 惡意軟體借助惡意的 Excel 附加元件進行傳播

據報導，JSSLoader 惡意軟體在最近活動中，透過惡意 Microsoft Excel .xll 附加元件進行發佈。JSSLoader 至少在 2019 年就為人所知，並與被稱為 Gold Niagara 威脅組織有關。JSSLoader 功能包括資料收集、下載任何有效酬載以及從 C&C 伺服器接收檔案與執行指令。

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.2

基於機器學習的防禦技術：

- 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。

2022/03/09

Gh0stCringe RAT 以易受攻擊的資料庫伺服器為目標

據報導，Gh0stCringe RAT 在最新活動中，針對易受攻擊的資料庫伺服器。Gh0stCringe也稱為 CirenegRAT，是基於舊 Gh0st RAT 公開原始程式碼的遠端存取木馬 (RAT) 變種。除了具有通常 RAT 功能外，Gh0stCringe 還可以用作其他有效酬載的下載器、鍵盤記錄器和剪貼簿資料竊取器。

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：

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

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。

2022/03/08

RagnarLocker 勒索軟體積極針對關鍵基礎設施企業

賽門鐵克安全機制應變中心團隊獲悉關於最新的勒索軟體變種 RagnarLocker 活動的 FBI 警報。根據該報告，各個關鍵基礎設施領域的 52 個企業，已被確定為該勒索軟體組織的受害者。RagnarLocker 勒索軟體於 2020 年 4 月首次被發現。已知該惡意軟體不會加密系統相關檔案夾預配置清單中的檔案，並會嘗試刪除受感染電腦上的磁卷陰影複製。

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
- Ransom.Gen
- Ransom.Hermes!gen2
- Ransom.Ragnarlocker
- Trojan.Gen.2

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18

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.Ragnarlocker Activity

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。

2022/03/08

惡意圾郵件行動夾帶惡意.PPAM附件來散布具有RAT功能的竊密惡意軟體：Agent Tesla

根據最近的一份報告，新的惡意郵件行動已經透過使用 .PPAM 檔（微軟 PowerPoint 使用的外掛程式檔）來傳遞 Agent Tesla 惡意軟體。在報告的行動過程中，惡意電子郵件被發送到各種目標，包括烏克蘭一家製造公司等。附在電子郵件中 .PPAM 檔含有惡意的巨集，並作為 Agent Tesla 有效籌載荷的植入程式。

近期觀察到的電子郵件主旨樣本：

- *NEW SHIPMENT // FOB // SHIPPER 2X40'HQ*
- *Urgent Purchase order - Feb22_765432*
- *Re: PROFORMA/COMMERCIAL INVOICE*
- *DHL Statement of Account & Overdue Invoices*

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!gen87
- ISB.Downloader!gen386
- ISB.Downloader!gen447
- Trojan Horse
- Trojan.Gen.NPE

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)。

基於機器學習的防禦技術：

- 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。

2022/03/07

惡名昭彰的 Anubis 繼續從 Android 用戶那裡竊取資訊

Anubis 是目前行動威脅領域中最熱門的銀行惡意軟體之一。這主要是因為其強大的功能，以及在各種駭客論壇和網站上可以免費獲得流出來的版本。該威脅能夠注入全球多達 228 家銀行和加密貨幣服務，最近幾天，7.0 版本在這些平臺上得到回應，包括社交媒體。賽門鐵克繼續監測 Anubis 的活動，我們預計在未來幾天會看到增加。

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：

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

2022/03/04

DanaBot 惡意軟體被用來針對烏克蘭國防部發動DDoS攻擊行動

根據一份最新報告，DanaBot 惡意軟體最近被用來對烏克蘭國防部的網頁郵件 (WebMail) 伺服器發起分散式阻斷服務 (DDoS) 攻擊。DanaBot 惡意軟體以惡意軟體即服務 (Malware-as-a-Service) 模式出售，其中聯合夥伴公司可購買已建置好包含 C&C 基礎架構及立即可用的惡意軟體使用權來投入攻擊行動。在報告的攻擊中，其中一個聯合夥伴公司使用 DanaBot 惡意軟體下載另一個用 Delphi 撰寫並包含 DDoS 功能的惡意執行檔。

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.Danabot
- Trojan.Gen.MBT

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。