保安資訊--本周(台灣時間2022/03/18)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 2.116 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/03/14)**

- 在**24萬300**台端點上，阻止了**1.082億**次嘗試掃描**Web**服務器的漏洞。
- 在**51萬1,500**台端點上，阻止了**4,510萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬5,500**台**Windows**伺服主機上，阻止了**2,490萬**次攻擊。
- 在**18萬5,600**端點上，阻止了**1,010萬**次嘗試掃描伺服器漏洞。
- 在**9萬8,900**台端點上，阻止了**500萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬8,200**台端點上，阻止了**400萬**次嘗試利用的應用程式漏洞。
- 在**43萬2,700**台端點上，阻止了**1,300萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,500**台端點上，阻止了**450萬**次加密貨幣挖礦攻擊。
- 在**13萬5,500**台端點上，阻止了**590萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,200**台端點上，阻止了**24萬2,900**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。

2022/03/17

巴西木馬針對葡萄牙使用者

我們知道最近有報導稱葡萄牙用戶成為巴西特洛伊木馬的目標。該惡意軟體通常透過社會工程網路釣魚電子郵件傳遞。感染方式依賴於多個下載階段來傳遞最終有效酬載。有效酬載包括多種功能，囊括銀行憑證的洩露和執行額外的惡意下載。

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.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

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

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。

2022/03/16

針對烏克蘭的假語言翻譯軟體

據觀察與 UAC-0056 威脅行爲者相關的惡意活動瞄準了烏克蘭。UAC-0056 或 UNC2589、TA471 與烏克蘭政府機關有關。該攻擊由一個編譯後的 Python 二進制檔案組成，該檔案偽裝成從攻擊者網站下載的烏克蘭語言翻譯軟件。GraphSteel 和 GrimPlant 的 Go 二進制檔案因假翻譯軟體的安裝而注入。然後惡意程式執行一系列偵察和憑證收集命令，設置登錄時執行下載器以實現其持續性。

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
- WS.Malware.1

2022/03/16

Pandora 勒索軟體進入威脅領域

根據報導，一種針對知名公司名為 Pandora 的新勒索軟體變種，在公共洩密網站上發布受害者詳細訊息。由於兩種惡意軟體之間的代碼相似，Pandora 勒索軟體被認為是 Rook 勒索軟體變種的名稱重定義或演變。勒索軟體將加密使用者資料並將 .pandora 副檔名附加到鎖定的檔案中。

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：

- Downloader
- WS.Malware.1

基於行為偵測技術(Snoar)的防護：

- SONAR.SuspLaunch!g18

2022/03/15

CaddyWiper -- 清除程式

根據最近的報導，已經觀察到另一個針對烏克蘭組織的清除程式。這個被稱為 CaddyWiper 的惡意軟體，有能力辨識該電腦是否為網域控制站並跳過這些電腦。這降低攻擊者在目標群組織內橫向移動的風險。

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.C

2022/03/15

瞄準烏克蘭的透過假冒防毒軟體更新散佈 Cobalt Strike 攻擊

烏克蘭的電腦緊急應變小組 (CERT) 發佈一份關於觀察到網路釣魚活動的聲明，該活動偽裝成烏克蘭政府機構的通知。誘餌是透過下載「關鍵安全更新」來提高網路安全的一種手段，這將使受害者在不知不覺中安裝假冒的 Windows 防毒更新，該惡意更新隨後將植入 Cobalt Strike 信標以及其他惡意軟體。

烏克蘭 CERT 小組提到，自 2021 年 12 月以來，觀察到許多網路釣魚散佈和網路入侵活動。

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.Cobalt
- Backdoor.Cobalt!gm
- 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已於第一時間收錄於不安全分類列表中。

2022/03/11

Escobar -- AbereBot行動惡意軟體的新變種

最近發現一種被稱為 Escobar的AbereBot 行動惡意軟體的新變種。據報導，該惡意軟體也在地下論壇上提供銷售。Escobar 的功能包括竊取敏感資訊和登錄憑證，以及發送、攔截或刪除簡訊。一些新功能包括從 Google Authenticator (Google的身分驗證程式可用來產生一次性密碼，以供 Google 或第三方服務進行雙因素身分認證) 竊取資料，或透過遠端遙控軟體「VNC Viewer」控制受感染的設備螢幕。

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.2
- AppRisk:Generisk

2022/03/11
Seedworm (又名MuddyWater) 發起一波提供 RAT 的新攻擊

Seedworm (又名 MuddyWater) 進階持續攻擊駭客集團，發起新一輪針對土耳其和其他亞洲國家機關組織的攻擊。據報導，這些行動是利用各式各樣的惡意郵件附件，來提供下載程式和一些遠端存取木馬 (RATs)，包括 PowerShell、Visual Basic 和 JavaScript。該集團最近利用 RAT 變種是一個名為 SloughRAT 基於 Windows 腳本檔案 (WSF) 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Hacktool
- Trojan Horse
- Trojan.Gen.2
- Trojan.Mdropper
- VBS.Downloader.Trojan

基於機器學習的防禦技術：

- 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。

2022/03/11
Pripyat 挖礦程式

地下市場、駭客論壇和網站充斥著加密貨幣惡意軟體和挖礦程式--對於集團和個人來說幾乎沒有找不到的駭客工具。Pripyat 也是這些選擇之一，最近在威脅領域中被觀察到，威脅者透過順道下載 (drive-by-download) 和盜版破解軟體提供它。

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!gen609

檔案型(基於回應式樣本的病毒定義檔)防護：

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

2022/03/11

攻擊者利用「網站聯絡表單」夾帶 BazarLoader -- 精密攻擊的前導程式

垃圾郵件行動是傳遞惡意檔案以滲入組織的傳統方式。然而，一些威脅行為者跳過常規，使用其他通信模式，如："網站聯絡表單" 來啟動與目標的聯繫。透過這種管道，檢測垃圾郵件運行的預防措施被繞過，一旦通信建立，合法的檔案共用服務，如：TransferNow 和 WeTransfer，可以被利用來傳遞 BazarLoader 有效籌載。

BazarLoader 通常是更複雜多階段惡意軟體攻擊的第一階段，通常用於部署 Conti 勒索軟體或 Cobalt Strike。

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 Horse
- 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。