保安資訊--本周(台灣時間2022/02/11)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 120 萬個受保護端點上總共阻止了 1.896 億次攻擊。這些攻擊中有 96% 在感染階段前就被有效阻止：**(2022/02/07)**

- 在**23萬3,600**台端點上，阻止了**1.010億**次嘗試掃描**Web**服務器的漏洞。
- 在**46萬5,000**台端點上，阻止了**3,510萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬3,800**台**Windows**伺服主機上，阻止了**2,380萬**次攻擊。
- 在**17萬9,500**端點上，阻止了**1,030萬**次嘗試掃描伺服器漏洞。
- 在**10萬4,100**台端點上，阻止了**480萬**次嘗試掃描在**CMS**漏洞。
- 在**14萬2,400**台端點上，阻止了**370萬**次嘗試利用的應用程式漏洞。
- 在**46萬2,800**台端點上，阻止了**1,230萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,100**台端點上，阻止了**340萬**次加密貨幣挖礦攻擊。
- 在**9萬5,500**台端點上，阻止了**450萬**次向惡意軟體**C&C**連線的嘗試。
- 在**7,500**台端點上，阻止了**22萬3,500**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。

2022/02/10

假冒 Windows 11 升級程式，暗藏 RedLine 竊密程式

利用微軟最近宣佈將 Windows 11 的升級開放給所有符合條件的裝置，網路攻擊參與者開始散佈偽造 Windows 11 升級安裝程式。網路攻擊參與者設置一個看似合法的網域名稱來誘騙用戶下載並執行 RedLine 惡意軟體。RedLine 為最廣泛的部署竊密程式之一，可以收集有關密碼、瀏覽器cookie、信用卡和加密貨幣錢包的資訊，因此其感染可能會對受害者產生可怕的後果。

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

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已於第一時間收錄於不安全分類列表中。

2022/02/10

Snatch (*搶奪) 勒索軟體

隨著 Snatch (*搶奪) 勒索軟體至少從 2019 年開始活動，如果受害者受到入侵後，攻擊者將進行橫向移動、竊取資訊、加密檔案，然後進行雙重勒索戰術--脅迫受害者，如果不支付贖金，將公開或出售從受害者那裡竊取的資訊。多年來，攻擊者利用暴力破解，垃圾郵件和已知漏洞來獲得初始入侵，但也試圖內神通外鬼僱用內部人員。

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：

- Ransom.Snatch!gm
- Ransom.Thieflock!gm

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Gen.MBT

- Trojan Horse
- Ransom.Snatch

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：

- Audit: Ransom.Gen Activity 55
- Attack: Ransom.Gen Activity 29

2022/02/09

NimbleMamba--新型惡意軟體，用於目標式垃圾郵件行動

最近發現名為 NimbleMamba 新型惡意軟體，針對阿拉伯語系國家使用者的垃圾郵件行動來散布。這些郵件包含諸如醫療警報新聞和有關地緣政治問題的資訊或機密資訊之類的誘餌，以誘使用戶點擊惡意RAR檔案鏈接。

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：

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

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。

2022/02/09

中國全運會系統被入侵破壞

研究人員發現，中國全運會的系統已被一個未透露姓名的中國駭客組織入侵。攻擊者最初透過利用已知 Windows 漏洞獲得存取權限。然後，攻擊者試圖透過上傳各種工具，利用已知的漏洞並上傳各種檔案類型來執行橫向移動，以識別可能會被攔截的工具。他們最終能夠透過上傳偽裝成 PNG 圖檔的新配置檔來重新配置網頁伺服器，然後上傳整個武器化的 Tomcat 伺服器。研究人員無法確定在遭駭期間竊取哪些資訊 (如果有的話)，並且在全運會開幕之前就解決。

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：

- Hacktool
- Trojan.Gen.NPE
- WS.Malware.1

基於安全強化政策(適用於使用DCS)：

DCS內建的強化安全政策早已針對伺服主機上的這些漏洞的零時差攻擊提供保護。

2022/02/09

TargetCompany (*目標公司) 勒索軟體

TargetCompany (*目標公司) 是一個勒索軟體集團，自 2021 年 6 月以來一直存在。加密檔案的副檔名大抵是 .mallox、.exploit、.architek 和 .brg 會因個案而異。

執行時，勒索軟體會採取一些措施來減輕其自身的惡意工作負載：

1. 為 SeTakeOwnershipPrivilege 和 SeDebugPrivilege 指定其程序
2. 刪除 vssadmin.exe、wmic.exe、wbadmin.exe bcdedit.exe、powershell.exe、diskshadow.exe、net.exe 和 taskkil 等特定工具的檔案執行選項
3. 使用以下命令刪除所有磁碟上的磁卷陰影複製：
   %windir%\sysnative\vssadmin.exe delete shadows /all /quiet
4. 重新設定開機選項：bcdedit /set {current} bootstatuspolicy ignoreallfailuresbcdedit
   /set {current} recoveryenabled no
5. 停用一些需要開啟重要檔案的程序，例如：資料庫：
   MsDtsSrvr.exe、ntdbsmgr.exe、ReportingServecesService.exe、oracle.exe、fdhost.exe、sqlserv.exe、fdlauncher.exe、sqlservr.exe、msmdsrv.exe、sqlwrite 和 mysql.exe

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.SuspLaunch!g18
- SONAR.SuspLaunch!gen4

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Gen
- Trojan.Gen.MBT
- Trojan.Gen.2
- Trojan Horse
- WS.Malware.1

基於機器學習的防禦技術：

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

2022/02/09

Medusa (*美杜莎) 利用簡訊騙局 (Flubot) 基礎設施散布

自從 2020 年以來，被稱為 Medusa (*美杜莎) Android銀行惡意軟體（具有遠端存取木馬--RAT功能）一直不斷進化，現在參與者一直在使用簡訊騙局 (Flubot) 大受歡迎的基礎設施來散布以擴大其覆蓋範圍。Medusa (*美杜莎) 使用系統的輔助服務功能，只需要少量的權限即可執行自動轉帳攻擊。「自動轉帳系統（Automatic Transfer System，ATS）」攻擊，允許參與者將資料輸入到合法網路銀行應用程式的欄位中。

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：

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。

- AppRisk:Generisk

2022/02/08

Vice Society (*邪惡社會)勒索軟體

不斷演變的網路威脅型態一定會有許多勒索軟體攻擊者，Vice Society (*邪惡社會) 最近幾個月相當活躍的攻擊者之一。他們的勒索軟體行動中，該駭客集團主要針對中小型公司。像其他惡名昭彰的勒索軟體集團一樣，他們也採用可怕的雙重勒索戰術來進一步向受害者施加壓力。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Heur.Dropper
- SONAR.SuspBeh!gen25
- SONAR.SuspBeh!gen526
- SONAR.SuspBeh!gen530
- SONAR.SuspBeh!gen625
- SONAR.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/02/08

PrivateLoader，按安裝付費的惡意軟體服務

PrivateLoader 是一種按安裝次數付費的惡意軟體即服務，營運商在其中提供付款，惡意有效籌載和目標資訊。營運商將散佈及傳遞酬載等工作外包，並根據感染次數來分潤。

散布通常透過網際網路搜尋引擎最佳化 (SEO) 下毒來進行，以誘使受害者下載並執行下載的惡意軟體。載入程式將與 C&C 伺服器報到，試圖用許多有效籌載來感染主機，例如：GCleaner、Raccoon、Redline、Smokeloader 或 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：

- Packed.Generic.528
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3
- WS.SecurityRisk.4

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。

2022/02/08

Vultur (*禿鷲) 活動仍然活躍，在 Google Play 商店上觀察到滴管／植入程式

Vultur (*禿鷲) 是一種具有遠端存取木馬 (RAT) 功能的 Android 銀行惡意軟體，至少從 2021 年初就開始存在。這種惡意軟體幕後主使者一直在使用名為 Brunhilda 的 Droper-as-a-Service (DaaS 滴管／植入程式即服務)，透過 Google Play 商店傳遞其威脅。截至今天，Vultur (*禿鷲) 仍然活躍，最近在 Google Play 商店上觀察到一個提供此惡意軟體的滴管／植入程式。滴管／植入程式是一個基於 Aegis 身份驗證應用程式開放原始碼的特洛伊木馬化之雙因子認證 (2FA) 應用程式。

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

2022/02/07

Roaming Mantis (*漫遊螳螂)：簡訊網路釣魚行動

Roaming Mantis (*漫遊螳螂) 是一種憑證盜竊和惡意散布行動，主要針對 Android 裝置，透過簡訊網路釣魚感染行動裝置惡意軟體。最近的攻擊顯示，除了日本、台灣和韓國之外，該攻擊者還針對歐洲（德國和法國）的用戶。

簡訊網路釣魚通常包含一個簡短的說明內容和一個網址 (URL)。用戶點擊網址時有兩種情況。一款適用於 iOS 用戶，一款適用於 Android 用戶。對於 iOS 用戶，他們會被重新轉址到模仿 Apple 官方網站提示輸入憑證的登錄頁面，而對於 Android 用戶，他們會被提示在他們的 Android 裝置上安裝 Android 應用 App。該 Wroba 惡意軟體偽裝成 Android 應用 App。該 Wroba 木馬的目標是竊取網路銀行詳細資訊，並進一步自動散布網路釣魚簡訊給受感染裝置聯絡簿中的人。

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