保安資訊--本周(台灣時間2022/12/23)
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 89 萬 2,500 台受保護端點上總共阻止了1.132億次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2022/12/19)**

- 在**16萬2,300**台端點上，阻止了**4,470**萬次嘗試掃描**Web**服務器的漏洞。
- 在**31萬6,200**台端點上，阻止了**2,420**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬2,000**台**Windows**伺服主機上，阻止了**1,720**萬次攻擊。
- 在**10萬6,500**端點上，阻止了**340**萬次嘗試掃描伺服器漏洞。
- 在**2萬9,800**台端點上，阻止了**150**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬9,700**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**29萬6,500**台端點上，阻止了**710**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**4,400**台端點上，阻止了**290**萬次加密貨幣挖礦攻擊。
- 在**4萬8,500**台端點上，阻止了**530**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,500**台端點上，阻止了**14萬6,000**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。

2022/12/22

開枝散葉～多種全新勒索軟體源於被洩露的Conti原始碼

已經在真實網際網路上發現多個源於遭洩露的 Conti 勒索軟體原始碼的新勒索軟體變種。發現的變種包括：Putin 勒索軟體、ScareCrow、Bluesky 和 Meow。雖然我們已經在八月份看到一些 Bluesky 樣本， 但最近才發現其他提到的勒索軟體家族。他們的特點包括：

- ScareCrow 加密使用者的檔案並為它們附加 .CROW 副檔名。勒索說明要求受害者透過 Telegram 與威脅者聯繫。
- Putin 勒索軟體會加密使用者的檔案並為其附加 .PUTIN 副檔名。該變種背後的威脅行為者還使用 Telegram 聯繫受害者。他們還在 telegram上公佈受害者的詳細資訊。
- Meow 加密使用者的檔案並為其附加 .MEOW 副檔名。勒索說明為威脅行為者提供電子郵件地址和 telegram 聯絡方式。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.Ransomware!g1
- SONAR.Ransomware!g7
- SONAR.Ransomware!g12

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Bluesky
- Ransom.Conti!gm1
- Ransom.Conti!gen4
- Ransom.Conti!gen10
- Ransom.Conti!gen12
- Ransom.Generic.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2022/12/22

助紂為虐～Nitol分散式阻斷服務(DDoS)惡意程式，助長Amadey殭屍電腦程式的散佈

在近期的多起攻擊行動中發現，Nitol 分散式阻斷服務 (DDoS) 惡意程式已被用來安裝 Amadey 殭屍電腦程式。Nitol 是一種眾所周知的 DDoS 惡意軟體，支援多種不同的 DDoS 攻擊任務。根據從 C&C 伺服器接收到的命令，惡意軟體還可能下載額外的有效籌載或進行更新。威脅

行為者可能會進一步使用在已揭露的攻擊行動中散佈的 Amadey 殭屍電腦程式從受感染的端點收集資訊或下載更多惡意籌載。

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：

- MSIL.Downloader!gen8
- 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：

- System Infected: Backdoor.Nitol Activity
- 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。

2022/12/21

鎖定土耳其安卓手機行動平台用戶～GodFather惡意軟體發動新一波攻擊行動

GodFather 安卓手機行動平台銀行惡意軟體在針對土耳其使用者的全新攻擊行動中捲土重來。這一次，惡意軟體透過偽裝成 MYT Müzik 應用程式的安裝程序進行散佈。GodFather 惡意軟體具有從受感染裝置竊取機密資料的功能，包括 SMS 簡訊內容、裝置詳細資訊和各種應用程式資訊。該惡意軟體還可能用於透過 VNC 操控螢幕並注入銀行網頁連結 (URL)。

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
- Android.Reputation.2
- AppRisk:Generisk

2022/12/21

又是移轉到Rust～Nokoyawa勒索軟體出現Rust程式語言的版本

在真實網際網路上發現基於 Rust 的 Nokoyawa 勒索軟體的全新變種。Nokoyawa 是一個勒索軟體家族，最早可追溯到 2022 年 2 月，最初是用 C 語言所撰寫。其他幾個勒索軟體變種已經移轉至 Rust 程式語言進行改寫，主要於更快的加密過程和更好的安全軟體規避能力。Nokoyawa 背後的威脅行為者還透過在進行加密之前盤查並過濾使用者資料來進行雙重勒索戰術。

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

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/12/20

透過釣魚網站散佈的DarkTortilla惡意軟體

DarkTortilla 惡意軟體最近透過偽裝成 Grammarly 和 Cisco 網站的網站釣魚頁面進行散佈。以前，DarkTortilla 曾透過帶有惡意附件的垃圾郵件廣泛傳播。在這個全新攻擊行動中，寄生在釣魚網站頁面上的惡意軟體植入程序偽裝成軟體安裝程序。執行後，安裝程序將向使用者顯示一則假訊息，通知應用程序由於相依文提性緣故而無法運行。DarkTortilla 有效籌載具有在受感染主機上建立持續性、聯繫 C&C 伺服器以接收更多命令以及下載其他有效籌載的功能。

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!gen45

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.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／IP位址已於第一時間收錄於不安全分類列表中。

2022/12/20

獵戶座～偽裝成網頁抓取工具的竊密程式

賽門鐵克最近觀察到偷渡式下載活動，其中攻擊者試圖用破解軟體和駭客攻擊來引誘受害者。受害者並不知情，他們實際上下載並執行了一個名為 Orion（也稱為 Orion 網頁抓取工具）的竊密程式。雖然作者將此惡意軟體宣傳為排名第一的抓取程式，但它幾乎是一個典型的竊密程式。以下是它的一些竊取功能：

- 網頁瀏覽器敏感資料（瀏覽記錄、cookie、密碼）
- 電腦訊息
- 桌面截圖
- 視訊圖片
- 加密貨幣剪貼簿竊密器（Clipper）

據作者稱，有 40 多個外掛可用，Orion 使用 Discord 的 webhook 向營運商回報。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/19

MCCrash殭屍網路對Minecraft私有伺服器發動DDoS攻擊

現在經過漫長等待後，你終於可以有 Minecraft 私服器可玩了，但是網站突然開始延遲，接下來就什麼也做不了。這可能是由於伺服器受到 DDoS 攻擊（由 MCCrash 發起）造成。根據最近的報導，這種威脅從 Windows 機器傳到 Linux 的設備，然後被其作者用於 DDoS Minecraft 私有伺服器，破解軟體是最初的感染媒介。

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：

- SMG.Heur!gen
- Trojan Horse
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/19

GoTrim瞄準網頁伺服器

GoTrim 是一個由 go 程式語言設計的殭屍電腦網路，其活動最近被曝光。主要用於掃描易受攻擊的內容管理系統 (CMS) 軟體並用於暴力破解。Web 伺服器一直是並且仍然是各種惡意軟體的目標，因為它們是大型惡意軟體發送的關鍵架構。GoTrim 背後的參與者很清楚這一點。

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.NPE

基於安全強化政策(適用於使用DCS)：

- 可疑執行程序： DCS 預防政策可防止惡意軟體在系統上被植入或執行。DCS 強化的 Linux 伺服器可防止從暫時或其他可寫入位置執行惡意軟體
- GoTrim bot 伺服器模式：DCS 預防政策針對任何傳入的 POST 請求阻止來自網際網路或 C&C 伺服器的傳入連接
- GoTrim bot 使用者端模式：DCS 預防政策阻止網際網路的傳出連接並限制來自伺服器的所需 HTTP 和其他流量

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。

2022/12/19

全新Venom遠端存取木馬(RAT)變種，新增竊密程式模組功能

近期 Venom 遠端存取木馬 (RAT) 的最新變種，新增竊密程式模組功能。該惡意軟體在地下論壇上出售，新版本的廣告中宣稱增加竊取密碼、cookie、書籤和儲存在瀏覽器中的自動填表資訊的功能。一旦收集到機密資訊，就會將其上傳至由攻擊者控制的 C&C 伺服器。除了竊密程式功能外，Venom 仍具有其先前版本中常見的典型遠端存取木馬 (RAT) 功能，包括啟動隱藏的 Explorer 和 PowerShell 對話、遠端鍵盤側錄器、Shell 命令執行、下載和執行任意檔案等。

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：

- AGR.Terminate!g2
- SONAR.ProcHijack!g45
- SONAR.SuspDataRun
- SONAR.SuspDrop!gen1
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- W32.Fixflo.B!inf
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/18

西班牙消費者和中小型企業遭受勒索軟體攻擊

儘管惡名昭彰的勒索軟體駭客集團因其對跨國大型組織造成的嚴重打擊而聲名大噪，但仍有許多較小的勒索軟體參與者在資安威脅版圖中低調發展 。例如：一個暫時默默無名的小勒索軟體被觀察到對西班牙語系的消費者和中小企業的個別電腦發動加密攻擊。加密後，檔案會被新增一個隨機的 4 個字元的副檔名和一則簡短的勒索贖金說明，要求支付相對可以接受的的 20 美元比特幣。沒有跡象顯示有採用雙重勒索戰術。

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.SuspDrop!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/18

巴西遭受BrasDex安卓手機平台銀行惡意軟體肆虐

最近觀察到另一種稱為 BrasDex 的 Android 手機行動平台銀行惡意軟體在巴西肆虐。其能夠執行自動轉帳系統 (Automatic Transfer System; ATS) 攻擊以竊取受害者的財務憑證。ATS 攻擊允許攻擊者在合法的網路銀行動APP和加密貨幣錢錢包的地址中輸入資訊，進而接手使用者的操作。據報導，這種威脅大約從一年前就開始活躍了，通常偽裝成與巴西銀行相關的 Android 手機行動平台應用程式。

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。

- AppRisk:Generisk

2022/12/16

利器被壞人運用就會成為凶器：Rust程式語言被大量運用於開發勒索軟體

Qilin 勒索軟體也被稱為 Agenda，以前被發現是採用 Go 語言所撰寫，然而，新版本被發現改採用 Rust 來撰寫。我們已經看到一些惡意軟體和勒索軟體改用 Rust 程式語言，以便更容易移植到不同的作業系統平臺，並試圖使其分析更加困難。Rust 版本似乎缺乏以前在 Go 版本中看到的一些功能，這可能意味著他們仍在開發和調整這個新版本，或者他們正試圖簡化或修改其操作。

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：

- Ransom.Qilin
- Ransom.Qilin!g1
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

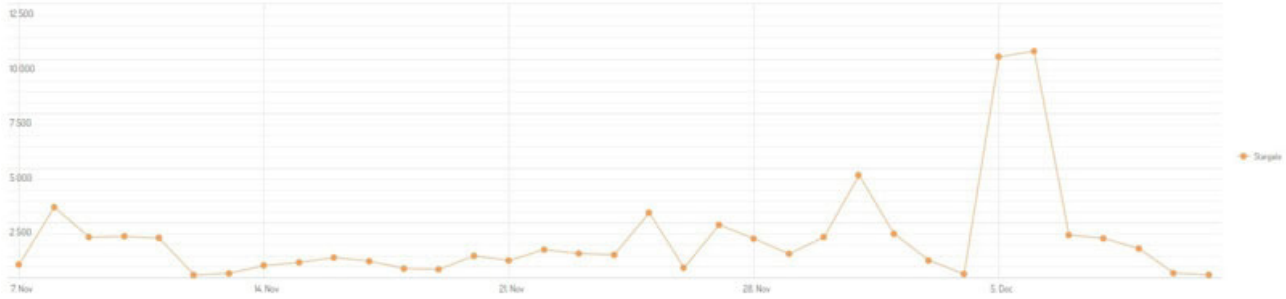
2022/12/15

防護亮點：即使採用混淆技術的的網路釣魚攻擊也不是賽門鐵克Stargate(*星際之門)安全引擎的對手

～防護亮點～

網路釣魚是最常見的社交工程攻擊之一，用於欺騙警覺性不足的人向攻擊者透露敏感資訊，以竊取機密及值錢的資訊，包括登錄憑證和信用卡號碼，受害者往往已經上鉤自己還不知道，並可能對受害者造成相當大的傷害。網路釣魚也是網路犯罪活動最常見的形式之一，特別是針對企業組織，網路釣魚攻擊在 2022 年顯著增加。地下市場上有大量的網路釣魚工具包可取得且價格便宜，賽門鐵克無時不刻都會攔阻新的網路釣魚攻擊。上周也不例外。

12 月 5 日，我們全天候的監控系統對暴增的惡意電子郵件流量發出警報。



經立即調查發現，我們的 Stargate (*星際之門) 安全引擎（由我們的電子郵件安全服務--Email Security Service簡稱：ESS所提供）憑藉其先進的啟發式威脅檢測能力，主動阻斷每一個暗度陳倉的電子郵件攻擊，其中隱匿經混淆化的程式碼（或在這種情況下試圖隱匿），伺機發動攻擊。一旦解除混淆並運行，該程式碼就會以 HTML 為目標，試圖透過網路釣魚來獲取和竊取微軟 Office 365 的登錄憑證和密碼。如果受害者被成功引誘，被盜資訊將被上傳到由攻擊者所控制的 C&C 伺服器，受害者就任人宰割了。

攻擊發動者竭盡全力以隱藏感染媒介以避免被發現，再加上通常會利用看起來完全合法的 "釣魚" 頁面或快顯視窗，毫無戒心的被攻擊目標幾乎不可能發現。幸運的是，賽門鐵克 ESS 客戶可以安然無恙，因為 "星際之門" 安全防護的進階啟發式引擎為他們做到這一點，足以讓攻擊者落荒而逃。

賽門鐵克擁有領先業界的 **零時差** 保護技術，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：

- Scr.Malscript!gen2

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)。

欲瞭解更多有關 Stargate--基於機器學習、雲知識和深度內容檢查的威脅檢測平臺的資訊，請在此聯繫 賽門鐵克。

2022/08/10

BlueSky (*藍天) 勒索軟體

BlueSky 是一個普通的勒索軟體集團，最近出現在已如過江之鯽的勒索軟體領域。在加密方面，他們的勒索軟體與 Conti 和 Babuk 等其他軟體有一些相似之處。根據多份報告，該勒索軟體似乎是透過瀏覽網頁的順道下載攻擊 (Drive-by-download) 所散佈發，目前該組織並未使用雙重勒索戰術 (先竊取再加密，勒索不成則公開竊取的資訊)。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g12

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Conti!gm1

基於機器學習的防禦技術：

- Heur.AdvML.B