保安資訊--本周(台灣時間2022/10/21)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 98 萬 600 台受保護端點上總共阻止了 1.337億次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2022/10/17)**

- 在**18萬1,400**台端點上，阻止了**6,260**萬次嘗試掃描**Web**服務器的漏洞。
- 在**33萬7,500**台端點上，阻止了**2,460**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬9,800**台**Windows**伺服主機上，阻止了**1,990**萬次攻擊。
- 在**12萬2,400**端點上，阻止了**530**萬次嘗試掃描伺服器漏洞。
- 在**4萬3,500**台端點上，阻止了**220**萬次嘗試掃描在**CMS**漏洞。
- 在**8萬3,000**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**32萬9,200**台端點上，阻止了**750**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,500**台端點上，阻止了**330**萬次加密貨幣挖礦攻擊。
- 在**5萬400**台端點上，阻止了**510**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,200**台端點上，阻止了**19萬9,900**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。

2022/10/20

Domestic Kitten進階持續威脅(APT)駭客組織，散播全新FurBall手機惡意軟體

被稱為 Furball 的手機行動平台惡意軟體的一個全新變種，已在針對伊朗公民的監視活動中被發現。據報導，該行動由 Domestic Kitten 進階持續威脅 (APT) 駭客組織 (也被稱為 APT-C-50) 所主導。雖然該惡意軟體的新版本與該惡意軟體家族早先的版本有許多相似之處，但它也對C&C通信和新的混淆方法更進一步優化。Furball 的功能包括對簡訊、聯絡人和通話記錄等的滲透前置作業。該惡意軟體還可能從 C&C 伺服器接收額外的命令。

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：

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
- Spyware:MobileSpy

2022/10/19

來自航運公司的電郵暗藏惡意程式嗎？

與航運業有關的社交工程攻擊已經存在了很長時間，雖然有些一看就知道事有蹊蹺，但如果加上該行業的知識與術語，還是會有一些成效的。多年來，我們已經看到多個團體和個人做了研究，瞭解了散貨船、集裝箱船和油輪。最近的一個例子是賽門鐵克觀察到一個全球的攻擊行動，利用熱門的的船舶名稱--海港輝煌號、海洋龍號、海洋寶石號、聯邦島號和大通雲帆號。如果成功地被惡意郵件引誘，用戶會在不知情的情況下執行一個假冒的 Formbook。

已觀察到的常見郵件主旨如下：

- MT HARBOUR SPLENDOR/03/ DISCHARGING PORT AGENT APPOINTMENT
- MV OCEAN DRAGON - DISCHARGE IRON ORE / AGENCY APPOINTMENT
- MV FEDERAL ISLAND CTM DELIVERY
- MV OCEAN GEMSTONE (V2201) // AGENT NOMINATION
- M.V //DA TONG YUN VOY// AGENCY NOMINATION FOR DISCHARGING WHEAT

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.Formbook
- Trojan.Gen.2
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/18

發現全新的變種Ducktail竊密程式

在真實網路環境發現全新的採用腳本程式語言 PHP 所撰寫的 Ducktail 竊密程式變種。Ducktail 首次出現在 2021 年鎖定臉書商業帳戶的惡意行動中。據報導，新的 Ducktail 變種主要透過免費或破解的應用程式和遊戲安裝程式傳播。新變種的功能仍然與原生版本相當類似，主要是竊取機敏資訊與登入等相關憑證。

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
- Infostealer.Ducktail
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

2022/10/18

透過TOAD(電話傳遞攻擊)散佈的Copybara手機行動平台上的惡意軟體

Copybara 也稱為 BRATA 的手機行動平台上的惡意軟體，在最近一波針對多家義大利銀行客戶的 TOAD（電話傳遞攻擊）攻擊中被傳播。威脅者一直在利用冒充義大利各金融機構網頁的釣魚網站。TOAD 攻擊涉及攻擊者和受害者之間的直接通話，受害者被說服在其設備上下載和執行惡意二進位檔案。Copybara 二進位檔案經常偽裝成假冒的安全性更新，而且該惡意軟體具有各種遠端存取能力。

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：

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

2022/10/18

在最近的攻擊行動中發現到 Spyder Loader 惡意軟體

賽門鐵克觀察到 CuckooBees 行動可能還在繼續進行中，這次是針對香港的組織。活動中觀察到的受害者是政府組織，攻擊者在一些網路上的活動時間長達一年之久。雖然我們在這次攻擊行動中沒有看到最終的有效籌載，但根據之前看到的與 Spyder Loader 惡意軟體一起被部署到受害者機器上的活動，看來這次活動的最終目的可能是收集情報。

在我們的部落格文章中有更多資訊可供參考：Spyder 載入器：最近在針對香港組織的活動中看到的惡意軟體

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：

- Trojan Horse
- Trojan.Spyload
- WS.Malware.1

2022/10/18

Cartel(*卡特爾)勒索軟體與Revil勒索軟體似乎有些相似

Cartel (*卡特爾) 勒索軟體是一個勒索軟體即服務 (RaaS) 營運模式下散佈的勒索軟體變種。這個惡意軟體第一次出現是在 2021 年 12 月，它與惡名昭彰的 Revil 勒索軟體表現出某種程度相似性。該勒索軟體背後的威脅者利用雙重勒索戰術，除了加密機敏檔案外，還脅迫受害者不付贖金就要公佈被盜資料。據報導，攻擊者在試圖入侵受害者時使用各種額外的工具，例如：DonPAPI、LaZagne 和 Mimikatz。

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!g19
- SONAR.Ransomware!g30
- SONAR.Ransomware!g39

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Cartel
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT

- WS.Malware.1
- 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／IP位址已於第一時間收錄於不安全分類列表中。

2022/10/17

土耳其的困擾--Formbook 惡意程式攻擊行動

賽門鐵克最近觀察到一個正在發動中 Formboo k惡意程式攻擊行動，主要針對土耳其的主要行業，包括以下行業：能源、運輸、食品和線上購物。威脅者自稱是一家鋁和碳纖維行業的知名土耳其公司，試圖用歷久不衰的 "訂單" 社交工程戰術（電子郵件主旨：Ynt: Sipari OnayI）來引誘受害者。這些惡意郵件帶有一個包含 Formbook 二進位的 .bz 檔案。這種惡意軟體至少從 2016 年就開始存在，截至今天仍然是真實網路世界的頂級竊密程式之一。

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)。

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/17

日本的Amazon Prime付費服務，用戶憑證面臨風險

年終假期即將來臨，網路犯罪分子非常清楚這是年度網路購物釣魚的最佳時機，而我們確實看到了一種上升趨勢。我們最近觀察到一個以 Amazon Prime 付費服務為主題的網路釣魚活動，其中有數千封電子郵件（主旨：亞馬遜プライムの自動更新設定を解除いたしました！番號）被發送給日本用戶。威脅者試圖誘使用戶相信他們 Amazon Prime 付費服務自動續約已被取消。如果使用者被這種社交工程戰術成功引誘，他們將被重新引導到一個虛假的亞馬遜登錄頁面，他們的憑證將被接管或遭竊。

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)。

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。

2022/10/17

老當益壯的NjRAT遠端存取木馬

NjRAT 是一個普通的遠端存取木馬，至少從 2013 年就開始存在，到今天為止，仍然被多個團體和個人有效運用。多年來，它的原始程式碼和變種在社交媒體、軟體發展和版本控制的代管服務以及駭客網站和論壇上獲得不計其數的迴響。消費者和企業都已成為惡意電子郵件和瀏覽網頁時的順道下載 (drive-by-download) 攻擊行動的目標，這些攻擊行動被偽裝成假冒的更新程式、破解軟體、原始遊戲提供改善模組和駭客工具。最近幾周，賽門鐵克觀察到威脅形勢出現了明顯的上升。

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：

- Backdoor.Ratenjay
- Backdoor.Ratenjay!gen3
- Downloader
- Trojan Horse

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/16

Venus(*維納斯)勒索軟體

最近，另一個被稱為 Venus 的普通勒索軟體被曝光，因為其背後的威脅者一直在針對公開曝險的遠端桌面服務。像許多勒索軟體一樣，一旦成功感染，它將試圖刪除陰影複製 (shadow copies) 並加密檔案 (加密後新增 .Venus 副檔名)。

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

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: NCrack Tool RDP BruteForce Activity
- OS Attack: RDP Scan Attempt 2

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/10/16

GuLoader 惡意程式以DHL相關的主題活動襲擊義大利和越南

GuLoader（又稱CloudEye）的流行程度忽高忽低，但顯然沒有任何停止的跡象。賽門鐵克每天都在觀察利用這種威脅載入各種遠端存取木馬和竊密程式的惡意郵件行動。最近，我們觀察到兩個以 DHL 為主題的行動，目標針對義大利和越南的組織，威脅者在郵件中附加了一個 ISO 檔案（年度熱門事件）。在 ISO 檔案中可以發現一個偽裝成 DHL 航空貨運提單（AWB）的惡意 VBScript，如果受害者被成功誘導執行它，就會觸發最終的有效籌載。

Email subject

- Dichiarazioni per importazioni richieste (1100549726 - SDOGANAMENTO)
- Khai báo cho hàng nhập khẩu bắt buộc (1100549726 - RÕ RÀNG HẢI QUAN

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.Gen.NPE