保安資訊--本周(台灣時間2022/04/08)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 2.149 億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/04/03)**

- 在**21萬8,200**台端點上，阻止了**1.125**億次嘗試掃描**Web**服務器的漏洞。
- 在**50萬**台端點上，阻止了**4,410**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**8萬5,300**台**Windows**伺服主機上，阻止了**2,660**萬次攻擊。
- 在**16萬1,000**端點上，阻止了**980**萬次嘗試掃描伺服器漏洞。
- 在**9萬700**台端點上，阻止了**480**萬次嘗試掃描在**CMS**漏洞。
- 在**12萬7,300**台端點上，阻止了**380**萬次嘗試利用的應用程式漏洞。
- 在**42萬2,100**台端點上，阻止了**1,170**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,200**台端點上，阻止了**440**萬次加密貨幣挖礦攻擊。
- 在**11萬9,100**台端點上，阻止了**640**萬次向惡意軟體**C&C**連線的嘗試。
- 在**6,800**台端點上，阻止了**23萬4,300**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。

2022/04/07

FFDroid -- 假冒合法應用程式偷偷竊取您的憑證 (帳密)

FFDroid 是一支竊密程式，目前透過假冒的“Telegram”應用程式來散布。一旦安裝後，FFdroid 會針對受感染裝置上的常見瀏覽器，竊取熱門社交媒體和電子商務網站的憑證(帳密)。

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

基於機器學習的防禦技術：

- Heur.AdvML.B

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(33246)

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。

2022/04/07

APT-C-23 駭客集團發動的 Bearded Barbie (*大鬍子芭比) 攻擊行動

在真實環境觀察到 APT-C-23 駭客集團發起的一項全新的大規模惡意行動，被稱為“Bearded Barbie (*大鬍子芭比) 行動”。據報導，攻擊者的目標是與執法、國防和緊急服務部門有關的以色列個人。在行動過程中，APT-C-23 一直在利用社交工程向受害者提供 Windows 和 Android 惡意軟體。Barbie 下載程式和 BarbWire 後門是該駭客集團現在使用的兩個全新且從未記錄過的惡意軟體變種。

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

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
- Android.Reputation.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。

2022/04/06

馬來西亞銀行用戶遭受到偽冒網路商店的詐騙攻擊

多家馬來西亞銀行的 Android 行動平台用戶，已成為透過社交工程戰術並假冒網路商店來竊取憑證的目標。攻擊發動者假冒提供家管服務和寵物用品等流行企業，透過建立以假亂真的網站和 Android 行動應用程式 (APP) 來欺騙受害者。

這些惡意 Android 行動應用程式 (APP) 仿效該服務並提示用戶選擇馬來西亞銀行進行付款。如果成功引誘，受害者將選擇他們的銀行並輸入他們的帳密，然後這些憑據將被攻擊者劫取。惡意 APP 還具有攔截和轉發簡訊功能，允許攻擊者接收銀行發送的雙重身份 (2FA) 驗證碼。

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：

- Android.Reputation.2
- AppRisk:Generisk

2022/04/06

Denonia 惡意軟體以 AWS Lambda-Serverless 的運算服務環境為目標

有報導稱，一種名為 Denonia 的惡意軟體，被精心設計專為在 AWS Lambda 環境（亞馬遜的 Serverless 運算服務，可以實現容器化服務的應用概念）中運行。以 Go 編寫，其最初的感染媒介尚未確定，但它的功能在記憶體中執行稱為 XMRig 的知名挖礦程式。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE
- Trojan.Horse

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。

2022/04/06

惡意垃圾郵件攻擊行動散布竊密程式：MetaStealer

最近發現一個正在進行中的惡意垃圾郵件攻擊行動，它傳播一個名為 MetaStealer 竊密程式。發動者利用典型的基金交易社交工程戰術以及惡意的 .XLS 檔案，該檔案啟動攻擊鏈以散布竊密程式，使用 Github 和 transfer.sh 來存放供下載的二進位檔案。

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：

- Downloader
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- Trojan.Mdropper

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。

2022/04/06

“閃電竊密程式”～讓人猝不及防嗎?

最近，一個全新基於 .NET 的竊密程式被揭露，它被稱為“閃電竊密程式”，正在透過網頁瀏覽時的順道下載傳播威脅。研究人員指出，雖然它的功能與其他常見的竊密程式非常相似，比較特殊是它以 JSON 格式儲存竊取的資料，以便滲出。

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

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。

2022/04/06

3LOSH 加密器用於傳播 AsyncRAT 和 LimeRAT 最新攻擊行動

在最近的一系列活動中，AsyncRAT和LimeRAT惡意軟體的有效籌載是透過含有惡意腳本的ISO磁碟鏡像檔傳遞的。負責這些攻擊的威脅集團一直在利用3LOSH加密器來混淆感染階段使用的惡意程式碼。攻擊者可以利用這兩個遠端存取木馬(RAT)系列獲得對被攻擊系統的控制權，並從這些系統中竊取機密資料。

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!gen10
- Downloader
- ISB.Downloader!gen76
- ISB.Downloader!gen281
- ISB.Heuristic!gen5
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- W97M.Downloader

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。

2022/04/05

不只是載入程式功能，Colibri也夾帶竊密程式：Vidar

Colibri 載入程式是一個主要針對Windows系統的隱蔽惡意軟體，早在 2021 年 8 月就首次出現在地下論壇。最近的一次惡意廣告行動發現，該載入程式現在投放了一個名為 Vidar 的竊密程式作為其最終的有效籌載。

賽門鐵克防護公告在 2021/10/11 發佈關於：在真實環境觀察到名為：Vidar 的資訊竊取活動

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：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- W97M.Downloader

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/04/05

由 Cicada (*蟬) 進階持續威脅 (APT) 組織發動的最新間諜活動

一個由中國國家支持的進階持續威脅 (APT) 組織正攻擊全球各地的組織，這可能是一場已經持續好幾個月的間諜活動。Cicada (*蟬--又名 APT10) 行動的受害者，包括全球多個國家的政府、法律、宗教和非政府組織 (NGO)，包括在歐洲、亞洲和北美。一旦攻擊者成功入侵受害者的電腦，他們就會部署各種不同的工具，包括客製化的載入程式及名為 Sodamaster 的後門程式。

賽門鐵克發佈以下部落格文章，其中包含更多詳細資訊：Cicada (*蟬)：中國進階持續性威脅 (APT) 集團在近期間諜活動中擴大目標

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
- Hacktool.Mimikatz
- Infostealer
- Trojan Horse
- Trojan.Dropper

基於機器學習的防禦技術：

- Heur.AdvML.C

基於安全強化政策(適用於使用DCS)：

賽門鐵克 Data Center Security (DCS) 針對 Microsoft Windows 和 Exchange 的強化政策可防止 APT10 所表現出的可疑活動，如部署 Mimikatz 工具進行憑證轉存。

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。

2022/04/05

一支全新的遠端存取木馬(RAT)出現在暗網市場，並以一部名為《Borat*波拉特》的模擬紀錄片命名

一支全新的遠端存取木馬 (RAT) 出現在暗網市場，並以一部名為《Borat* 波拉特》的模擬紀錄片命名。RAT 是一種允許攻擊者獲得對受害者機器的管理控制的工具，但與其他 RAT 變種不同，Borat 也可以被利用來進行勒索軟體和DDOS活動。

其他功能包括：

- 鍵盤側錄--監測和記錄按鍵，並將其儲存在一個 txt 檔案中
- 勒索軟體--在受害者的電腦上部署勒索軟體的有效籌載，並透過波拉特自動產生贖金說明
- DDoS--透過使用被攻擊機器的資源將垃圾流量導向目標伺服器
- 音訊錄製--透過麥克風錄製音訊，如果可用的話，並將其存儲在 wav 檔中

- 網路攝像頭記錄--從網路攝像頭記錄視頻，如果可用的話
- 遠端桌面--啟動一個隱藏的遠端桌面來執行檔操作、使用輸入裝置、執行代碼、啟動應用程式等。
- 反向代理--設置一個反向代理，以保護遠端操作員的身份不被暴露
- 設備資訊--收集基本的系統資訊
- 進程空洞化--將惡意軟體代碼注入合法進程以逃避檢測
- 憑證竊取--竊取存儲在基於 Chromium 的網路流覽器中的帳戶憑證
- Discord權杖竊取--從受害者那裡竊取 Discord 權杖
- 其他功能--透過播放音訊、交換滑鼠按鈕、隱藏桌面、隱藏工作列、按住滑鼠、關閉顯示器、顯示空白螢幕或掛起系統來擾亂和迷惑受害者。

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
- Trojan.Gen.2
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/04/04

Redline 竊密程式在駭客圈嶄露頭角

威脅領域有許多竊密程式，長期以來，熱門的家族沒有什麼變化，但最近幾個月，Redline竊密程式的熱門程度越來越高。根據賽門鐵克對日常活動的持續觀察，這種公開的惡意軟體現在是全球多個團體和個人使用的頂級資訊竊取者之一。雖然我們看到許多針對企業和消費者的攻擊通透許多感染媒介，但電子郵件和順道下載仍然是使用最多的伎倆。

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!gen25
- SONAR.SuspDataRun

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：

- Packed.Generic.525
- Packed.Generic.616
- Trojan.Gen.2
- Trojan.Gen.MBT

基於機器學習的防禦技術：

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

2022/04/04

UAC-0056 威脅集團，持續攻擊烏克蘭

據報導，UAC-0056威脅集團（也被稱為 SaintBear 或 TA471）發起的一個新惡意攻擊行動，利用帶有惡意巨集的 Excel 檔案的魚叉式網路釣魚電子郵件。這個威脅發動者的持續攻擊是針對烏克蘭的組織。攻擊鏈可拆解為多個階段，攻擊者利用基於 Go 的植入程式和下載程式及 GrimPlant 和 GraphSteel 等後門。

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.2
- W97M.Downloader
- 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。

2022/04/01

Deep Panda 進階持續威脅 (APT) 組織利用 Fire Chili rootkit 惡意軟體

據報導，名為 Deep Panda 進階持續威脅 (APT) 組織以 VMware Horizon 伺服器為攻擊目標，利用 Log4Shell 漏洞，試圖提供後門和一種被稱為 Fire Chili 的新 rootkit 惡意軟體。該 rootkit 被發現是用偷來的憑證進行數位簽章，其目的是為了隱藏被入侵系統上的惡意元件存在來規避偵測。

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.Trojan
- Hacktool.Rootkit
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於行為偵測技術(Snoar)的防護：

- SONAR.Module!gen3

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: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2

基於安全強化政策(適用於使用DCS)：

賽門鐵克 Data Center Security (DCS)內建的入侵防禦 (IPS) 系統能有效防禦 VMWare Horizon 伺服器的 Log4Shell 漏洞攻擊並提供零時差保護。

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。

2021/10/11

在真實環境觀察到名為：Vidar 的資訊竊取活動

已在真實環境觀察到被稱為 Vidar Stealer 資訊竊取惡意軟體的新活動。該資訊竊取惡意軟體至少從 2018 年就開始為人所知，並且可以在各種地下論壇上出售。Vidar Stealer 的目標是竊取瀏覽器相關資料，例如：cookie、瀏覽器歷史記錄或存儲的憑證，但它也可以從加密貨幣錢包、FTP、電子郵件或聊天應用程式中擷取資訊。在最近的活動中，已經觀察到 Vidar 背後的威脅行為者濫用 Mastodon 社交網路，並配合當前 C&C 命令與控制伺服器。

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(基於病毒定義檔)防護：

- Heur.AdvML.B
- Packed.Generic.620
- Trojan Horse

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已於第一時間收錄於不安全分類列表中。