保安資訊--本周(台灣時間2022/12/16)
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 92 萬 5,100 台受保護端點上總共阻止了1.167億次攻擊。這些攻擊中有 92% 在感染階段前就被有效阻止：**(2022/12/12)**

- 在**16萬6,100**台端點上，阻止了**4,800**萬次嘗試掃描**Web**服務器的漏洞。
- 在**32萬1,600**台端點上，阻止了**2,450**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**6萬3,400**台**Windows**伺服主機上，阻止了**1,740**萬次攻擊。
- 在**10萬6,600**端點上，阻止了**330**萬次嘗試掃描伺服器漏洞。
- 在**2萬8,600**台端點上，阻止了**150**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬8,800**台端點上，阻止了**200**萬次嘗試利用的應用程式漏洞。
- 在**32萬4,600**台端點上，阻止了**800**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬5,400**台端點上，阻止了**320**萬次加密貨幣挖礦攻擊。
- 在**5萬800**台端點上，阻止了**540**萬次向惡意軟體**C&C**連線的嘗試。
- 在**4,700**台端點上，阻止了**14萬7,800**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。

2022/12/15

影像監控系統傳播～RedGoBot分散式阻斷服務(DDoS)攻擊殭屍網路

基於 Go 語言撰寫的 RedGoBot 分散式阻斷服務(DDoS)攻擊殭屍網路已經被揭露。此威脅背後的攻擊發動者能夠透過 HTTP、UDP 和 TCP 洪水攻擊發起分散式阻斷服務 (DDoS) 攻擊。最重要的是，它還能夠清除原先已經入侵在該裝置上的其他 DDoS 殭屍電腦的程序。據報導，RedGoBot 正在透過已知的 Vacron (台灣馥鴻科技) 影像監控系統遠端程式碼執行 (RCE) 漏洞進行傳播。

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

2022/12/14

Lokibot在電子郵件領域的崛起

在這一點上，Lokibot 是大多數人都知道的竊密程式，它已經在資安威脅版圖嶄露頭角多年，現在流行率仍然很高。這種威脅已被用於竊取憑證和加密貨幣錢包，但也被用作部署第二階段惡意軟體的後門。最重要的是，它負責暗網上無數的憑證轉存(credential dumps)。

賽門鐵克持續每天觀察活動，但在過去幾週，我們發現惡意垃圾郵件活動有所增加。這些惡意垃圾郵件活動不使用時髦或花哨的社交工程手法，相反地，威脅發動者採用普通的報價、運輸、SWIFT、出貨明細及發票和支付相關的社交工程主旨。

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!g21

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.2
- 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：

- System Infected: Bad Reputation Process Request 4

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/14

遍地開花～Teng Snake(*騰蛇)勒索軟體，Chaos原始碼被公開後的後起之秀

自從 Chaos 勒索軟體開放原始碼可由公共資源方便取得之後，它湧現出無數變種，這些變種由世界各地的駭客組織和個人所操弄。Teng Snake 勒索軟體是最近在資安威脅版圖中觀察到的變種之一。根據受害者機器上呈現的贖金說明，該威脅攻擊者並未採用雙重勒索手段，並且索價 10,000 Tether虛擬貨幣 (約合 10,000 美元)。被加密後的檔案其附檔名通常會是四個隨機字串。

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.SuspLaunch!g18

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

2022/12/14

伊朗駭客組織Cobalt Mirage的攻擊行動，駭客運用名為Drokbk的惡意軟體

今年年初有報導稱，Cobalt Mirage 的攻擊行動中，攻擊者利用惡名昭彰的 Log4j 漏洞作為初始感染媒介。一旦入侵成功後，一個名為 Drokbk 的後門會被植入，它使用 Github 作為固定情報投放點解析器(Dead Drop Resolver)。該組織至少從 2020 年開始活躍，主要針對西方組織 (美國、以色列、歐洲、澳大利亞)。今年年初，勒索軟體活動也與該組織有關。

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: Log4j2 RCE CVE-2021-44228
- Attack: Log4j2 RCE CVE-2021-44228 2
- Attack: Log4j CVE-2021-45046
- Attack: Log4j CVE-2021-45105
- Audit: Log4j2 RCE CVE-2021-44228

基於機器學習的防禦技術：

- Heur.AdvML.C

2022/12/13

Harly繼續偷偷入侵Google Play商店

與 Joker 類似，Harly Android 訂閱者繼續偽裝成常用APP (例如：臉部編輯、自拍APP) 進入 Google Play 商店。這種威脅對惡意軟體營運商來說可能非常有利可圖，對受害者的財務也極具破壞性，因為在不知不覺中從 Google Play 商店下載並安裝 Harly 用戶將訂閱一系列付費性服務。

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

2022/12/13

刀俎魚肉～BByStealer竊密程式視遊戲玩家和Discord為魚肉

在過去幾個月中，多個駭客組織和個人使用了另一個普通的 Discord 竊密程式 (BByStealer)。觀察到的透過瀏覽網頁時的偷渡式下載攻擊行動證實，遊戲玩家和 Discord 用戶一直是 BByStealer 的主要鎖定目標。這個竊密程式的氾濫主要是因為它的程式碼可以在公共資源上方便獲得，例如：用於軟體開發和版本控制的熱門網路代管平台。BByStealer 將 Discord 登錄、加密錢包和網路瀏覽器與許多其他通用竊取功能打包在一起。

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：

- Suspicious: content
- Trojan.Gen.MBT
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2022/12/13

再起風雲～LokiLocker加密勒索軟體再傳災情

今年年初發現的 LokiLocker 加密勒索軟體是以惡意軟體即服務 (Ransomware-as-a-Service) 的營運模式繼續在資安威脅版圖中嶄露頭角。該勒索軟體背後的攻擊者仍然採用逾時不付贖款就會刪除檔案，以進一步迫使受害者支付贖金。被加密後的檔案其附檔名並沒有規則可循，現況看到的案例都不太一樣。

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.Cryptlck!g171
- SONAR.Heur.Dropper
- SONAR.Ransomgen!gen3

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

2022/12/12

AESRT勒索軟體

AESRT 是另一種在真實網路情境發現的普通勒索軟體。被該惡意軟體加密後的檔案其附檔名為 .AESRT。被該而且並沒有提出贖金說明，而是彈跳出視窗，其中包含攻擊者的聯繫訊息以及用於輸入解密密鑰的欄位。AESRT 勒索軟體確實具有刪除電腦上的磁卷陰影複製的功能。

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.SuspLaunch!g18
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

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

2022/12/12

魚目混珠～Zombinder服務被濫用於將Ermac竊密程式與合法應用程式綁定

在真實網路情境發現到針對 Android 和 Windows 平台的新惡意攻擊行動。攻擊者一直在傳播Android 平台上的 Ermac 銀行木馬和 Windows 平台上的 Erbium、Aurora 和 Laplas 竊密程式。該

惡意軟體已經透過謊稱 Wi-Fi 熱點自動身份驗證的 APP 或瀏覽器更新程式的虛假網站進行散佈。一旦用戶被引誘下載並執行該 APP，它就會在受感染的裝置上安裝最終的有效籌載。該攻擊行動幕後的威脅組織一直在利用第三方服務，該服務用於將混淆的惡意籌載與名為 Zombinder 的 Android 平台上的APP綁定。

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
- Trojan.Gen.MBT

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.1
- Android.Reputation.2
- AppRisk:Generisk

2022/12/09

利用Truebot殭屍電腦的全新攻擊行動

在最近針對竊密程式和勒索軟體散佈的攻擊行動中觀察到 Truebot 惡意軟體。該惡意軟體屬於俄羅斯駭客組織 Silence 所操控，據信該組織與 APT 攻擊者 TA505 有關。Truebot 散佈的媒介會因不同的攻擊行動而異。8 月份的早期攻擊利用資產管理工具 Netwrix Auditor 的 RCE 漏洞 CVE-2022-31199。近期攻擊行動透過 USB 裝置使用 Raspberry Robin 惡意軟體感染來傳播有效載荷。Truebot 是一種下載程式變種，負責收集系統資訊並將額外有效籌載下載到受感染的端點。

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：

基於行為偵測技術(Snoar)的防護：

- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.2
- 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：

- 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。

2022/12/09

惡意簡訊攻擊行動～鎖定印度銀行客戶進而散佈手機行動平台惡意程式

已經觀察到針對印度銀行客戶的全新惡意簡訊攻擊行動。攻擊者利用虛假的銀行網站，這些網站提供積分兌換優惠券或現金。這些網站冒充 HDFC、Axis 或 SDI 等知名銀行的入口網站。在一些相關的攻擊行動中，威脅行為者還一直在使用“Know Your Customer”(KYC) 身份驗證樣板從事詐騙，以凍結帳戶為由來誘騙用戶進行緊急驗證。這些攻擊行動中散佈的惡意軟體具有收集客戶的銀行詳細資訊和憑證 (帳號密碼) 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：

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

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。

2022/12/09

小心你的雲端帳密～AndroxGh0st惡意軟體鎖定AWS…等帳密

AndroxGh0st 是一種基於 Python 的惡意軟體，與名為 Xcatze 的威脅攻擊發動方有所關聯。該惡意軟體實際上是一個 SMTP 破解程式，用於讀取 Laravel Web 應用程式框架暴露的 .ENV 檔案，以獲取配置資訊，包括 AWS、O365、SendGrid、Twilio 等的憑證(帳號密碼)。AndroxGh0st 包含各種功能，包括利用被公開揭露的憑證(帳號密碼）和 API，但它也可以部署 webshell。

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.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- MSIL.Downloader!gen7
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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：

- Audit: Environment Config File Download Attempt
- Web Attack: Androxgh0st Scan Attempt

基於安全強化政策(適用於使用DCS)：

- 可疑程序執行：預防策略防止惡意軟體在系統上被植入或執行。
- DCS 強化使用 Laravel 應用程式的自定義沙箱，可以幫助保護 .ENV 檔案不被利用。
- 已知該腳本會將輸出寫入特定檔案目錄--這也可以透過 DCS 預防策略來預防。

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。

2022/12/08

Backshow勒索軟體

在過去的幾週裡，一個名為 Backshow 的全新勒索軟體集團已在資安威脅版圖嶄露頭角，它採用雙重勒索戰術，儘管此時與其他駭客集團相比它的泛濫程度及知名度都較低。一旦在系統上成功執行，它將為受害者建立一個單獨的編號 (ID) 並將其附加到加密檔案中。

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：

基於行為偵測技術(Snoar)的防護：

- AGR.Terminate!g2
- SONAR.SuspLaunch!g18

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

2022/12/08

防護亮點：惡馬惡人騎，胭脂馬遇到關老爺～Formbook難逃賽門鐵克郵件安全服務(ESS)的手掌心

～防護亮點～

難以置信電子郵件問世數十年後，還能成為主要的溝通工具，尤其在企業中。我們可以看到電子郵件的流行，每天有數千億封電子郵件發送到世界各地，因此它也成為垃圾郵件發送者的頭號目標。根據您的來源，估計目前發送的所有電子郵件中大約有一半到四分之三以上是垃圾郵件。這些垃圾郵件中的絕大多數是“malspam”，也就是包含或傳遞惡意軟體的垃圾郵件。

2016年出現的 Formbook 原本是一隻鍵盤側錄木馬，但是後來被發現功能強大，被用於發動大規模垃圾郵件感染全球企業。這也是最惡名昭彰的竊密程式之一，它搞得我們天昏地暗。大家對於Formbook 耳熟能詳的事蹟如下：

- Formbook 使用**電子郵件**作為其主要感染媒介，但也可能使用驅動下載、漏洞利用工具包和軟體漏洞
- 使用一系列令人眼花繚亂的電子郵件主旨，但似乎更喜歡相當普通的“支付”類型的社交工程戰術，包括虛假訂單電子郵件、運輸和 SWIFT外匯轉帳
- 至少從 2016 年開始，一直是最常見的竊密惡意程式和表單劫持惡意程式
- 主要目的從瀏覽器收集憑證並收集螢幕截圖和點擊或鍵盤側錄
- 有能力下載和執行額外的惡意檔案
- 負責暗網上的大量憑證轉存
- 以惡意軟體即服務 (MaaS) 的形式出售，並被世界各地的多個駭客組織和個人所採用
- 針對許多不同的行業和業務部門以及全球多個地區和國家部署有針對性和無針對性的攻擊行動

惡馬惡人騎，胭脂馬遇到關老爺～Formbook 難逃賽門鐵克郵件安全服務(ESS)的手掌心
對過去幾週我們的全球情資網路遙測大數據的分析顯示：
超過一萬封與 Formbook 相關的惡意郵件
針對多個地區和行業的多個攻擊者和攻擊行動
使用數百個電子郵件主旨的數十個攻擊行動
所有這些威脅都被賽門鐵克郵件安全服務(ESS) 的惡意軟體掃描元件**主動攔截阻止**。

賽門鐵克郵件安全服務 (ESS) 客戶請放心，我們卓越並深受信任的郵件安全技術將替你為贏得勝利做好準備。『好』還不夠好。卓越才會給你帶來成果。卓越才會為你帶來競爭優勢。卓越才能勝出。

要了解有關賽門鐵克雲端郵件安全服務的更多資訊，**請點擊此處下載我們型錄及簡報檔**。