
# 保安資訊--本周(台灣時間2023/08/25)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 65 萬 1,600 台受保護端點上總共阻止了 7,840 萬次攻擊。這些攻擊中有 84.1% 在感染階段前就被有效阻止：**(2023/08/21)**

- 在**13萬2,000**台端點上，阻止了**3,000**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**20萬5,300**台端點上，阻止了**1,620**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬9,500**台**Windows**伺服主機上，阻止了**1,240**萬次攻擊。
- 在**8萬5,800**台端點上，阻止了**220**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,900**台端點上，阻止了**80萬200**次嘗試掃描在**CMS**漏洞。
- 在**6萬5,300**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**22萬9,900**台端點上，阻止了**550**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,600**台端點上，阻止了**200**萬次加密貨幣挖礦攻擊。
- 在**14萬900**台端點上，阻止了**1,060**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**9萬3,100**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。

## 2023/08/24

## Metabase存在驗證前遠端程式碼執行漏洞(RCE)：CVE-2023-38646

CVE-2023-38646 是上個月被揭露的一個嚴重等級 (CVSS 評分：9.8) 遠端程式碼執行漏洞 (RCE)，影響熱門的商業智慧 (Business Intelligence；BI) 平台：Metabase。該漏洞會影響 0.46.6.1 之前的版本 (開放原始碼) 和 1.46.6.1 版 (企業版) 的 Metabase。如果該漏洞被開採利用，未經身份驗證的遠端攻擊者可能會在該伺服器提權來執行任意指令。

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：

**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: Metabase RCE Vulnerability CVE-2023-38646

---

## 2023/08/24

## SmokeLoader駭客組織的攻擊行動正在傳播Whiffy Recon惡意軟體

SmokeLoader 駭客組織最近攻擊行動傳播一種名為 Whiffy Recon 的 Wi-Fi 掃描惡意軟體。電腦一旦感染被植入 Whiffy Recon，就會被偵測系統上是否存在 WLANSVC 服務 (無線自動配置服務)。如果找到，它將開始濫用 Windows WLAN API 掃描附近的 Wi-Fi 存取點。收集需的資料將發送到 Google 地理位置定位 (Geolocation) API 服務，該服務允許攻擊者將受感染系統的位置三角測量到特定的地理坐標。由於掃描活動每分鐘發生一次，因此可以有效地跟踪受感染的系統。

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(SONAR)的防護：**

- SONAR.ProcHijack!g45

**檔案型(基於回應式樣本的病毒定義檔)防護：**

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

**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。

## 2023/08/24

## 以人工智慧(AI)工具為幌子的竊密程式正透過臉書的廣告傳播

隨著當前大型語言模型 (Large Language Model，LLM) 的流行，網路上歹徒也利用這一趨勢來引誘受害者 (在本例中是透過刊登人工智慧 (AI) 工具和服務付費的臉書廣告），也就不足為奇了。如果受害者點擊該廣告，攻擊者將濫用合法網址 (URL) 轉導向歹徒所操控的網站或雲端硬碟，以下載受密碼保護的壓縮案。密碼保護目的是避免被安全軟體檢測到，因為它內部包含 Windows installer 檔。如果用戶繼續，就會安裝一個虛假的瀏覽器瀏覽器外掛／擴充，歹徒將透過該外掛／擴充嘗試從受害者那裡竊取盡可能多的資訊，特別是與臉書 (Facebook) 相關的所有資訊。

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：

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1

**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。

---

## 2023/08/24

## 是雙頭蛇嗎？DarkGate(又名 MehCrypter)：既是加密軟體也是竊密軟體

DarkGate (又名 MehCrypter) 於 2018 年首次被發現，當時透過 BT 種子檔 (torrent ) 傳播。現在推出新版本，並採用惡意廣告和購買搜尋引擎排名 (SEO 中毒) 來傳播。感染規則和功能與以前的版本相同，該惡意軟體既是『加密程式』又是『竊密程式』，後者功能包括鍵盤側錄、剪貼簿竊密程式和竊取加密貨幣錢包等。

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：

**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.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。

## 2023/08/23

## Spacecolon工具集被濫用於發動Scarab勒索軟體攻擊

Spacecolon 是一個惡意軟體工具集，用於傳播 Scarab 勒索軟體，最近一些攻擊行動歸因於被稱為 CosmicBeetle 的駭客集團。該工具集由三個不同的模組（安裝程式、駭客工具和服務模組）所組成，允許攻擊者在遭入侵的系統上執行任意命令以及下載和執行其他惡意籌載。據報導，CosmicBeetle 駭客集團還在攻擊中使用各種其他工具，包括紅隊工具。

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(SONAR)的防護：**

- AGR.Terminate!g2
- SONAR.SuspBeh!gen625

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- 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
- 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。

---

## 2023/08/23

## 老奸巨猾的Agniane(*阿尼安)竊密程式

Agniane 是最近發現的竊密惡意程式，透過 Telegram 進行推廣，並以惡意軟體即服務 (MaaS) 產品的形式進行廣告銷售。歹徒利用此竊密程式竊取系統資訊、憑證、cookie、瀏覽器存儲的資訊和加密貨幣錢包等。Agniane 竊密程式是採用 C# 程式語言所撰寫，採用各種反分析和規避技術，包括沙箱檢測、反逆向檢查、混淆等。Agniane 收集的機密資料被洩漏並上傳資料至歹徒所操控的 C&C 伺服主機。

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(SONAR)的防護：**

- SONAR.MalTraffic!gen1
- SONAR.TCP!gen1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

**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 568
- System Infected: Trojan.Backdoor Activity 656
- System Infected: Trojan.Backdoor Activity 721
- 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。

## 2023/08/22

### 防護亮點：賽門鐵克防護超越國界--日本正遭受境外沒完沒了的日文化網路釣魚電子郵件

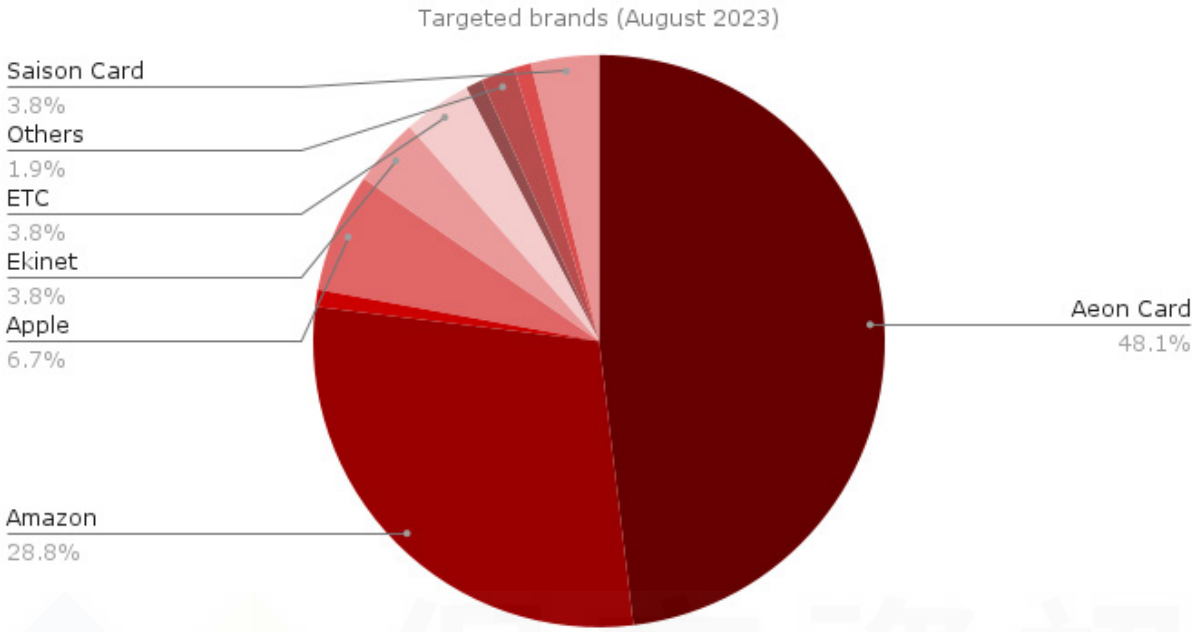
日本消費者和企業用戶每天都不斷受到大量惡意電子郵件的轟炸，這些電子郵件的伎倆是透過網路釣魚獲取機敏資訊和 (或) 進行詐騙，常會因此而導致身份盜竊、財務損失、帳戶接管、魚叉式網路釣魚等。多年來這些沒完沒了的攻擊，幕後的歹徒一直聲稱自己是日本網際網路最常使用的服務--通常與信用卡等金融服務相關。

儘管這些駭客集團和個人大多數並非來自日本當地，但這些惡意電子郵件有越來越多是用日語編寫，語法和拼寫水準也存在不同程度的差異；假冒的網站也是如此。這一增長可歸因於翻譯服務水準的不斷進步。

隨著這些工具越來越厲害，特別是人工智慧 (AI)，網路上的歹徒能夠輕鬆地將其網路釣魚內容翻譯成目標語言，使其對潛在受害者來說顯得更加真實。這不僅幫助他們克服語言障礙，還使他們能夠根據特定地區和人口統計數據來客製化內容，使網路釣魚內容更具說服力。然而，由於以下幾個原因，他們仍然難以準確翻譯這種具有獨特語法結構和復雜細微差別的文化情境語言：

- 禮貌用語和敬語
- 平假名、片假名和日本漢字
- 上下文和歧義
- 文化差異
- 語法和詞序
- 缺乏並行資料

以下圓餅圖概括說明賽門鐵克本月觀察到日本網路釣魚被鎖定的服務商。




如此圓餅圖所示，亞馬遜和 Aeon 用戶是最有針對性的服務。然而，我們也觀察到其他目標，例如：Apple、NTT、SMBC、AU、EPOS、ETC、Ekinet、Saison 卡、美國運通和三越伊勢丹等。此外，犯罪分子主要濫用 .cn、.shop 和 .cfd 頂級域名來建立欺詐性域名。

觀察到的電子郵件主主旨例（按原樣--包括拼寫錯誤）：

- Amazonプライム会費のお支払い方法に問題があります
- えきねっとにシステムを更新する
- えきねっとサービスご利用者様へ大切なお知らせ
- 三井住友銀行アカウントの異常通知
- [AMERICAN EXPRESS] ご請求金額確定のご案内
- 「ETC利用照会サービス」アカウントの有効性を検証する必要がある
- Apple IDの監視：非常に重要なお知らせ
- 三菱ＵＦＪ会社から緊急のご連絡
- セゾンカード: 一瞬で終わる安全確認をお願いします！
- 【SMBCからの大切なお知らせ】ネットショッピングご利用時の本人認証方式変更のお願い
- 【SAISONカード】ご利用確認のお願い
- Aeon Payアカウントでの異常な取引が検出されました。

賽門鐵克的多重防護技術已經於第一時間提供最有效的保護(**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。

欲瞭解更多有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。
欲瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

## 2023/08/22

## 不要安裝來路不明的應用程式～XLoader的macOS最新版本以OfficeNote應用程式為幌子傳播

XLoader 是源於知名的老牌竊密程式：Formbook 經改編並重新命名的全新惡意軟體變種。其主要威脅是竊取憑證、網路瀏覽器 cookie 和資訊、記錄遭入侵系統上的鍵盤輸入歷程以及竊取其他類型的用戶機敏資訊。macOS 上的版本是在 2021 年左右才出現，並以 Java 應用程式的形式傳播。將 XLoader 傳遞到 macOS 系統的最新攻擊行動將惡意軟體檔案偽裝成名為『OfficeNote』的常用商用軟體。該應用程式已捆綁到 .dmg 的蘋果磁碟映像檔中，並最初使用有效的數位簽章，但該簽章已被撤銷。一旦部署，該惡意軟體就會常駐並開始收集剪貼簿資訊和存儲在各種網路瀏覽器中的資訊等。

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：

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- WS.Malware.1

## 2023/08/22

## Carderbee進階持續性滲透攻擊(APT)駭客集團

Carderbee 是一個前所未聞的進階持續性滲透攻擊 (APT) 駭客集團，濫用合法的 Cobra DocGuard 檔案保護 (加密) 軟體來發動供應鏈攻擊，其作用是將 Korplug 惡意後門程式 (又名 PlugX) 部署到受害者電腦上。在此攻擊過程中，攻擊者使用帶有合法 Microsoft 數位簽章的惡意軟體。該攻擊行動的受害者以香港居多，也有一些在亞洲其他地區。

在我們的部落格文章中有更多資訊可供參考：Carderbee APT 集團針對香港機構發動濫用合法軟體的供應鏈攻擊。

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(SONAR)的防護：**

- AGR.Terminate!g2
- SONAR.TCP!gen6

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Downloader
- Hacktool
- Trojan Horse
- Trojan.Dropper
- Trojan.Gen.MBT
- WS.Malware.2

**基於機器學習的防禦技術：**

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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。

---

## 2023/08/18

## 初試啼聲就驚豔：專門攻擊商用企業級路由器的HiatusRAT遠端存取木馬惡意程式(RAT)

HiatusRAT 是一支相對較新的遠端存取木馬惡意程式 (RAT)，常見於針對商業等級和企業等級的路由器攻擊行動中。該惡意軟體於今年首次被發現，允許攻擊者可遠端操控遭入侵的設備、設置 SOCKS5 代理、擷取路由器的封包與流量、下載並執行從遠端 C&C 伺服器下載的檔案並執行惡意腳本等。除了原先已經支持的 MIPS、MIPS64 和 i386 之外，最近偵測到的最新版本還相容於多種 CPU 架構，包括 ARM、Intel 80386 和 x86-64。最新的攻擊行動以鎖定美國和台灣為多。

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：**

- Downloader
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

**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。

## 2023/08/18

## 更改帳密這麼重要的事不會(該)只是透過電郵通知啦～Zimbra郵件協作系統用戶遭受針對式網路釣魚行動攻擊

最近偵測到針對拉丁美洲和歐洲 Zimbra 郵件協作系統用戶的網路釣魚攻擊行動。該釣魚郵件偽裝來自 Zimbra 系統管理員所寄發的通知信，警告被害者，除非他們點擊鏈接或打開附加的 HTML 檔案並輸入其憑證／帳密，否則他們的帳號將會被停用。電郵本文中的鏈接和所附 HTML 中的表單目標都指向『zimbraAdmin.php』檔案以進行憑據／帳密竊取。

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：**

- Phishing.HTM.Gen

**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。