
# 保安資訊--本周(台灣時間2023/12/22)
# 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 60 萬 5,800 台受保護端點上總共阻止了 5,880 萬次攻擊。這些攻擊中有 78.9% 在感染階段前就被有效阻止：**(2023/12/18)**

- 在**10萬6,500**台端點上，阻止了**1,720**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**17萬3,800**台端點上，阻止了**1,440**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬1,400**台**Windows**伺服主機上，阻止了**1,080**萬次攻擊。
- 在**6萬3,700**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,800**台端點上，阻止了**70萬2,800**次嘗試掃描在**CMS**漏洞。
- 在**4萬7,100**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**23**萬台端點上，阻止了**410**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,030**台端點上，阻止了**240**萬次加密貨幣挖礦攻擊。
- 在**11萬8,900**台端點上，阻止了**940**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**782**台端點上，阻止了**30萬4,000**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。

## 有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 1.446 萬個受保護端點上阻止了總計 630 萬次攻擊。**(2023/12/18)**

- 使用網頁信譽情資，在 **1.293** 萬個端點上阻止 **550** 萬次攻擊。
- 攔截 **30K** 個端點上 **588.8K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **12.3K** 個端點上攔截 **166.6K** 次瀏覽器通知詐騙攻擊。
- 在 **547** 個端點上攔截 **46K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 **1K** 個端點上阻止 **2.4K** 次技術支援詐騙攻擊。
- 在 **240** 個端點上阻止 **911** 次加密劫持嘗試。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

## 2023/12/21

## 盜版的OnlyFans手機APP被發現暗藏SpyNote多功能竊密程式

OnlyFans(OF) 是全球知名情色平台，又有成人版 IG 之稱，過去幾年在全球的受歡迎程度呈指數型增長。作為一種社交媒體服務平台，它已成為許多網紅、小模、YouTuber 賺錢的新途徑與手法。然而，尺度與內容的拿捏，在藝術與色情範疇根本很難界定。用戶坐享該平臺潛在收益的同時，如果沒有拿捏得當，更可能會導致得不償失。

在這種數位環境下，網路犯罪分子已將 OnlyFans 的內容創造者和使用者視為一個不可多得目標。賽門鐵克發現，從網路釣魚到電腦以及手機上的惡意軟體，攻擊形式推陳出新反復出現。最近，我們發現有人試圖透過一款聲稱可以存取 OnlyFans Premium 高資費服務的手機 APP 來引誘使用者。這個冒名加料的惡意 APP 提供獨特的獨家體驗，為用戶提供迷人的照片、互動視訊以及來自有影響力人士和名人的專家建議。實際上，它根本就是一個不實的晃子--它實際上是 SpyNote 多功能竊密程式。

這種兼具間諜軟體／遠端存取木馬的惡意威脅在全球氾濫成災，其原始程式碼早已被公開。就功能而言，它可以收集鍵盤記錄、設備資訊、連絡人、通話記錄、簡訊內容、照片和影片，以及已安裝 APP 的相關資訊。它還能自行錄音通話內容和拍照、錄影。

受騙上當又缺乏保護軟體的使用者，很可能不僅會成為身份和財務盜竊的受害者，而且還會成後續被勒索的受害者。此外，他們的連絡人也可能面臨進一步的風險。

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.1

---

## 2023/12/21

## 陳年老舊的MS Office漏洞CVE-2017-11882仍被開採濫用於傳播竊密惡意軟體：Agent Tesla

看到 CVE-2017-11882 年序就知道這是一個陳年老舊的安全漏洞，影響 Microsoft Office 中的公式編輯器元件。成功開採濫用該漏洞可能會讓攻擊者在受感染的電腦上遠端執行程式碼。據觀察，Agent Tesla 是一個惡意軟體家族，在最近一些攻擊行動中仍在開採濫用這個陳年老漏洞。初始感染鏈由包含 CVE-2017-11882 漏洞的 .xlam 附件之惡意郵件所開啟。一旦漏洞被開採濫用，後續感染鏈就會衍生到惡意 VBS 和 JPG 檔、PowerShell 腳本和 DLL 二進位檔案涉入的後續階段，最終導致傳遞 Agent Tesla 的最終有效籌載。

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：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.Powershell!g85
- SONAR.SuspBeh!gen667
- SONAR.SuspDataRun
- SONAR.TCP!gen1

**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
- Exp.CVE-2017-11882!g2
- Exp.CVE-2017-11882!g3
- Exp.CVE-2017-11882!g5
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE

- Trojan.Sorcurat
- WS.Malware.1

**基於機器學習的防禦技術：**

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

**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。

## 2023/12/21

## 部落格發布系統Movable Type API CVE-2021-20837漏洞正在被大肆開採利用

CVE-2021-20837 是一個影響部落格發布系統 Movable Type API 嚴重等級的 (CVSS 風險評分 9.8) 命令注入漏洞。如果成功被開採濫用，此漏洞可遠端執行程式碼。賽門鐵克的網路入侵防禦 (IPS) 根據威脅狀況監控進行掃描，結果顯示最近開採濫用該漏洞的情況有所上升。雖然該漏洞已公開揭露好幾年，但攻擊者希望利用企業延遲部署修補的空窗期來得利。

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：

- Attack: MovableType RCE CVE-2021-20837

## 2023/12/20

## GuLoader惡意軟體下載器涉入的大規模網路攻擊行動： 從首爾到布魯塞爾

GuLoader 惡意軟體下載器的氾濫程度依然不減，賽門鐵克持續在全球範圍內觀察其涉入的網路攻擊行動。其中一個特殊案例引起我們的注意，因為該惡意行動者的行為讓人聯想到農地慘遭蝗蟲過境，作物無一倖免。事實上，在過去的三周裡，該攻擊者已經在韓國策劃三波大規模攻擊行動，最近又將重點轉移到比利時。

在韓國活動中，網路攻擊者一直假冒韓華工程建設公司（Hanwha Engineering & Construction），以韓國的能源、製造、遊戲、物流和製藥行業為目標。惡意電子郵件（主旨：한화건설 캐나다 온타리오주 프로젝트 견적 요청）包含一個 7z 壓縮檔，內含 GuLoader 被偽裝成一份虛假的 PDF 訂單檔案。

至於最近在比利時觀察到的活動，就受害者而言，它們目標行業包括保險、建築、諮詢、軟體工程、人力銀行、金融、藝術和能源。與韓國的情況類似，其作案手法仍然如出一轍，電子郵件（主旨：RFQ December/Last quarter order-19122023）包含一個惡意的 7z 壓縮檔，其中 GuLoader 二進位檔案被偽裝成一個偽造的 PDF 文件檔。

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)。

**基於行為偵測技術(SONAR)的防護：**

- ACM.Ps-Wscr!g1
- ACM.Wscr-Ps!g1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Trojan.Gen.NPE

**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
- System Infected: Trojan.Backdoor Activity 719

---

## 2023/12/20

## Xray(*X光) 勒索軟體

Xray 是在威脅環境中觀察到另一種勒索軟體，其目標是公司的伺服器和用戶端電腦。從功能上看，它是一種通用的勒索軟體，允許網路歹徒決定加密哪些資料夾，跳過哪些資料夾不加密。加密成功後，會被冠上 .Xray 的副檔名。

根據隨附提供的勒索 (贖金支付) 說明檔案的內容 (Xray_Help.txt)，沒有明確的證據顯示他們是否採用雙重勒索手法，也沒有指定贖金金額。他們只是建議使用者透過電子郵件聯繫他們。目前，該攻擊發動者並不像其他更活躍的勒索軟體惡棍那樣猖獗。不過，賽門鐵克還是持續對其活動保持高度警戒。

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：**

- ACM.Ps-RgPst!g1a
- ACM.Ps-Schtsk!g1
- SONAR.Dropper

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.Generic.1

## 2023/12/20

## 冒名墨西哥郵政(Correos De Mexico，像台灣中華郵政)網路釣魚行動正在上演

賽門鐵克發現新一波冒名墨西哥郵政 (Correos De Mexico，像台灣的中華郵政) 以竊取憑證／帳密的網路釣魚行動。電子郵件內容非常具體，提到一個未交付的包裹。未交付包裹的原因是『尚未完成繳交關稅』。為了使電子郵件內容看起來真實和個人化，網路釣手在送貨單明細內加入收件人的電子郵件地址。點擊該電子郵件中顯示的釣魚網址後，受害者就會進入設好圈套的憑據／帳密收集釣魚網頁。

主旨：En caso de impago, Su paquete será retenido！
主旨意思：如果不付款，您的包裹將退回寄件者。

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：

**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。

---

## 2023/12/20

## 新版IDAT惡意程式載入器，被TA544駭客組織濫用於近期的攻擊行動

據報導，TA544(又名 Narwal Spider) 進階持續威脅滲透組織在真實網路情境發動一連串新的惡意網路活動。據瞭解，該頑強駭客組織過去曾鎖定義大利多個組織和機構為目標。在最近的攻擊行動中，攻擊者利用 IDAT 惡意程式載入器 (Loader) 的新變種來傳播 Remcos 遠端存取木馬 (RAT) 或 SystemBC 惡意軟體等各種有效籌載。

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：**

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

**基於機器學習的防禦技術：**

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

**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。

## 2023/12/20

## 同時支援 Windows／macOS的JaskaGO惡意竊密程式

JaskaGO 是一款 GO 程式語言撰寫的惡意竊密程式，同時支援 Windows 和 macOS 平臺。該惡意軟體會從遭入侵的電腦收集大量資料，包括憑證、cookies、瀏覽器歷史記錄、本地資料夾中的檔案、密碼錢包等。搜刮到的資料會被壓縮成一個 .zip 壓縮檔，並上傳到攻擊者所遭控的 C&C 伺服器上。除了資訊竊取功能外，JaskaGO 還能執行從攻擊者處接收的 shell 命令，並下載和執行其他有效籌載。

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：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- Heur.AdvML.C

---

## 2023/12/20

## Splunk正式揭露存有遠端程式碼執行(RCE)漏洞--CVE-2023-46214

CVE-2023-46214 是最近被揭露影響 Splunk Enterprise 平臺的遠端程式碼執行 (RCE) 漏洞。由於在處理使用者提供的可擴展樣式表語言轉換 (XSLT) 時存在漏洞，遠程攻擊者可能能夠上傳惡意 XSLT，導致在受影響的 Splunk 實例上執行遠端程式碼。該漏洞的開採濫用程式碼已被公開釋出，建議用戶升級到 Splunk 9.0.7 和 9.1.2 或更高版本以修復此問題。

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: Splunk RCE CVE-2023-46214

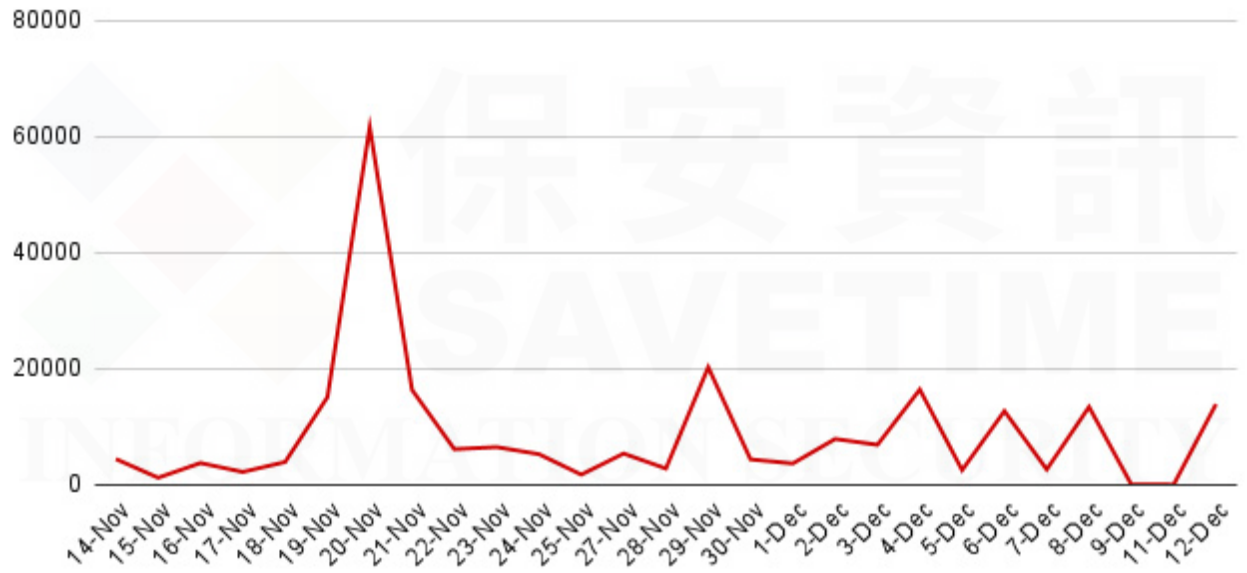
## 2023/12/19

### 防護亮點：祝福的季節--謹防禮券和獎勵計畫詐騙

正值年終節慶期間，禮品卡和獎勵計畫詐騙猖獗。這是永遠不會退流行的騙術，至今在全世界仍被廣泛使用，特別是在禮券和禮品銷售旺季前後更是明顯增加。這些惡意禮券和獎勵計畫詐騙通常屬於網路釣魚攻擊的範疇。它們通常利用人性貪圖免費贈品和優厚折扣的弱點。

具體情況如下：網路釣手會傳送誘人的資訊，誆稱你抽中了某知名品牌的免費禮券或某些特別獎勵。一旦有人上鉤，點擊連結或按照他們的指示操作，用戶可能會被要求提供個人資訊或下載含有惡意軟體的檔案。有些人甚至會誘騙用戶先付款以領取他們的『免費』禮物。這是一種典型的誘騙行為，讓受害者兩手空空，敏感資訊也可能洩露。

賽門鐵克掌握大量的攻擊行動，最近幾周出現的大量釣魚網頁數量 (超過28萬～283k) 引起我們的注意。以下是我們觀察到的與該行動相關的釣魚網頁數量。




這些釣魚網頁上架在 294 個最近才註冊的域名的網站，這些域名似乎是運用 DGA(動態網域產生演算法) 來混淆視聽，顧名思義，網域清單會動態不斷的隨機產生。這些域名稱使用不常見的頂層網域名 (TLD)，例如：beauty、boats、bond、cfd、fun、homes、lat、monster、sbs……等。範例如下：

- masonblackwell[.]beauty
- harmonyx[.]cfd
- jayleo[.]bond
- nebulashift[.]boats
- eliwhitestudio[.]monster

這類社交工程騙術和攻擊通常是針對消費者，但企業用戶受到的影響也不小。事實上，私人與公務上的上網界線已變得越來越模糊。員工在辦公時間使用公司電腦，可能也會不小心落入設局圈套，給公司的基礎設施帶來巨大風險。

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

**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。

建議客戶啟用 WebPulse 即時分類功能，以獲得最佳保護。請點擊此處獲取配置 WebPulse 說明。
欲深入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。
欲深入瞭解更多有關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。

---

## 2023/12/19

## Zimbra郵件協作系統存在跨網站腳本(XSS)漏洞：CVE-2023-37580

CVE-2023-37580 是最近被揭露的一個影響 Zimbra 郵件協作系統的零時差漏洞 (CVSS 風險等級評分：6.1) 跨網站腳本(XSS)漏洞。成功開採濫用該漏洞後，攻擊者可透過注入惡意腳本來破壞目標系統的機密性和完整性。該漏洞的開採濫用程式碼已被公開釋出，也有人回報在真實網路情境傳出災情。建議用戶升級到 8.8.15 Patch 41 或更新的版本來修復此漏洞。

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: Zimbra Collaboration XSS CVE-2023-37580

**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。

---

## 2023/12/19

## Play(*播放)勒索軟體--企業面臨的最新攻擊

賽門鐵克安全機制應變中心 (Symantec Security Response) 團隊瞭解到最近美國國土安全部網路安全暨基礎設施安全局 (CISA)、聯邦調查局 (FBI) 以及澳洲通訊情報局 (Australian Signals Directorate，ASD) 轄下的澳洲網路安全中心相繼發布資安警報：Play(又名 PlayCrypt) 勒索軟體的一連串攻擊行動。Play 勒索軟體早在 2022 年 6 月就已被發現，自那時起，它已涉入多起引人注目的攻擊。據報導，賽門鐵克追蹤到營運該勒索軟體幕後的駭客集團名為 Balloonfly，在最近的攻擊行動鎖定北美、南美和歐洲的眾多企業和國家級關鍵基礎設施。攻擊者一直在濫用客製化

開發的 .NET 工具 Infostealer.Grixba 以及其他多種駭客工具，包括 Cobalt Strike、SystemBC、GMER、IOBit、PowerTool、Mimikatz 等。與其他勒索軟體集團類似，Play 幕後主使者也採用雙重勒索手段，在加密資料之前還會先從受害者網路中竊取並回傳資料。

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：

**基於行為偵測技術(SONAR)的防護：**

- ACM.Untrst-RunSys!g1
- AGR.Terminate!g2
- SONAR.RansomGen!gen3
- SONAR.RansomPlay!gen1
- SONAR.RansomPlay!gen2
- SONAR.RansomPlay!gen3
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7
- SONAR.TCP!gen1
- SONAR.TCP!gen6

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.SystemBC
- Downloader
- Infostealer.Grixba
- Ransom.PlayCrypt
- Ransom.PlayCrypt!g1
- Ransom.PlayCrypt!g2
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

**基於機器學習的防禦技術：**

- Heur.AdvML.A!300
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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: Bad Reputation Process Request
- System Infected: Trojan.Backdoor Activity 568

**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。

## 2023/12/19

## 以『你不在家』通知為幌子的Evri網路釣魚電子郵件正在瘋傳

Evri 是一家英國的包裹運送廠商。隨著年終節慶購物旺季的到來，出現偽裝成 Evri 包裹通知的詐騙電子郵件正在瘋傳。這些電子郵件以『你不在家』為幌子，誘使用戶點擊釣魚網頁以重新安排送貨時間。這些釣魚網頁是架構在被劫持的域名的網站，其唯一目的就是竊取憑據／帳密。

郵件主旨： 約定下次送貨時間。

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。

---

## 2023/12/19

## Apache OFBiz存在遠端程式碼執行(RCE)漏洞：CVE-2023-49070

CVE-2023-49070 是 Apache OFBiz(Open for Business，是一套功能齊全的企業自動化套件) 中的一個嚴重等級 (CVSS 評分：9.8) 預設授權存在遠端程式碼執行漏洞 (RCE)。成功開採濫用該漏洞後，攻擊者就可以完全控制伺服器，進而竊取敏感性資料、破壞運營系統，甚至對組織網路發起進一步攻擊。賽門鐵克的網路入侵預防系統的技術 (IPS) 可阻止這些漏洞利用嘗試，防止系統受到進一步感染／入侵。

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: Apache Ofbiz RCE CVE-2023-49070

## 2023/12/19

## 伊朗駭客集團--Seedworm，鎖定非洲的電信機構發動攻擊行動

博通公司 (Broadcom) 旗下的企業安全部門～賽門鐵克威脅獵手團隊最近觀察到由 Seedworm 駭客集團針對北非和東非電信組織所發動的網路攻擊行動。這次攻擊行動發生在 2023 年 11 月，濫用一些歸屬於 Seedworm 駭客集團的現有及新增駭客工具。C&C 是架構在最近披露 MuddyC2Go 的 C&C 專用框架。涉入攻擊的其他元件包括各種遠端存取工具、公開可用的 Venom Proxy 駭客工具的定製版以及定制的鍵盤側錄器。

在我們的部落格文章有更多內容，歡迎參閱：伊朗駭客集團--Seedworm，鎖定非洲東北部的電信機構發動攻擊行動。

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：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.TCP!gen6

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.Trojan
- Hacktool
- Trojan Horse
- WS.Malware.2

**基於機器學習的防禦技術：**

- Heur.AdvML.A

**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。

---

## 2023/12/18

## Vortex(*渦流)竊密惡意程式

賽門鐵克全天候監控新的竊密惡意程式時，發現一名網路惡棍為名為 Vortex 的竊密惡意程式建立 Telegram 頻道。在追蹤相關線索後，發現似乎是於發動攻擊行動時也同時進行相關測試。該惡意軟體與許多竊密惡意程式大同小異，都是透過濫用 Discord 和 Telegram 向該行動惡棍回報並竊取資訊。

Vortex 能夠竊取敏感的瀏覽器資料、Discord 權杖、Telegram 會話、加密貨幣錢包、Minecraft 和 Roblox 相關檔案、遊戲會話（Epic、Steam 等）、系統資訊以及電腦目錄中，包含以下不區分大小寫字串的文件檔 (小於 2MB)：

- password(*密碼)
- secret(*秘密)
- account(*帳戶)
- tax(*稅)

- key(*金鑰)
- wallet(*錢包)
- backup(*備份)

被盜資訊將被壓縮打包並上傳到 Gofile 或 Anonfiles；惡意軟體還會使用網路鉤子將其發佈到作者的 Discord 上。它還能透過 Telegram 機器人發佈到 Telegram 上。這種情況取決於作者有效籌載的配置。一旦上傳前述壓縮打包，它就會從遭入侵的電腦上刪除。

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：**

- ACM.Ps-Enc!g1
- ACM.Ps-Reg!g1
- ACM.Untrst-FlPst!g1
- SONAR.Dropper
- SONAR.Stealer!gen1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Infostealer
- ISB.Malscript!gen9

**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: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 634

---

## 2023/12/15

## JinxLoader惡意程式載入器：大肆買廣告宣傳並在真實網路情境出現

JinxLoader 是由 Go(Golang) 程式語言所撰寫新型惡意程式載入器，最近在地下論壇上非常流行。報告顯示，它最近被用於惡意電子郵件，載入 Formbook 等威脅。該惡意軟體向《英雄聯盟》角色 Jinx(吉茵珂絲) 致敬，其廣告海報和 C&C 登錄面板上都有該角色。就字義來看，JinxLoader 的主要功能非常直截了當，就是載入惡意軟體 (Loader)，被他感染後就會楣運當頭 (Jinx)。

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.MBT

**基於機器學習的防禦技術：**

- Heur.AdvML.B!200
- Heur.AdvML.C

---

## 2023/12/15

## MetaMask加密貨幣錢包使用者成為網路釣手新一波覬覦的目標

最近賽門鐵克發現新一波利用虛假驗證通知欺騙 MetaMask 用戶的網路釣魚行動。電子郵件內容提供一個截止日期，並提到如果不進行驗證，『未驗證』帳戶將被暫停。它誘使用戶點擊網頁以驗證其 MetaMask 錢包。

**保安補充網路知識**：MetaMask 是用於與以太坊區塊鏈進行互動的加密貨幣錢包。它可以透過瀏覽器擴充功能或行動應用程式手機 APP 讓使用者管理其以太坊錢包，與去中心化應用進行互動。MetaMask 由 ConsenSys Software Inc. 開發運營，主要專注於以太坊為基礎的工具及基礎設施。

電子郵件主旨：

- 主旨 您的 MetaMask 錢包將被暫停使用
- 寄件者："MetaMask"<chief@redacted_domain>

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。

---

## 2023/12/15

## Apache Struts漏洞CVE-2023-50164已在真實網路情境被開採濫用

CVE-2023-50164 是最近被揭露一個影響 Apache Struts2 開源 Web 應用程式框架的嚴重等級 (CVSS風險評分9.8) 路徑遍歷漏洞。如果成功開採濫用該漏洞，攻擊者可進行路徑遍歷並導致遠端代碼執行 (RCE)。該漏洞的開採濫用概念性驗證 (PoC) 程式碼已被公開發佈，該漏洞也有在真實網路情境被開採濫用的回報案例。建議用戶升級到 Struts 2.5.33 或 Struts 6.3.0.2 或更高版本，以修復此問題。

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: Apache Struts2 RCE CVE-2023-50164

---

## 2023/12/15

## Pandora(*潘朵拉)hVNC遠端存取木馬(RAT)在真實網路情境持續傳出災情

Pandora hVNC 是一種遠端存取木馬 (RAT)，自 2021 年以來就一直存在於威脅環境中，它能讓攻擊者遠端控制受感染的電腦。除主要的 RAT 功能外，該惡意軟體還具有鍵盤側錄、下載和執行任意有效籌載以及遠端命令執行等竊密程式的功能。Pandora hVNC 的新變種經常在網路犯罪論壇上進行宣傳和銷售。

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!gen6
- SONAR.SuspBeh!gen633
- 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.Reputation.1
- 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!100
- Heur.AdvML.B!200
- Heur.AdvML.C

## 2023/12/15

## 不輸兔子的烏龜～Turtle(*烏龜)勒索軟體～專挑文件檔案加密

一種被稱為 Turtle 或 TurtleRansom 的新型勒索軟體在真實網路情境已經有災情回報。該惡意軟體帶有針對各種平臺（包括 Windows、Linux 和 macOs）的不同版本。該惡意軟體主要針對文件類型的檔案進行加密（副檔名為 .doc、.docx 或 .txt 的檔案），所以很快就會造成災損。加密成功後，它會在被加密的檔案冠上『.TURTLERANSv0』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：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.TCP!gen1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Linux.RansomTurtle
- Ransom.Turtle
- OSX.RansomTurtle
- OSX.Trojan.Gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.Reputation.1

**基於機器學習的防禦技術：**

- Heur.AdvML.A!500
- Heur.AdvML.C