
# 保安資訊--本周(台灣時間2022/08/12)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 96 萬 4,300 個受保護端點上總共阻止了1.645億次攻擊。這些攻擊中有 94% 在感染階段前就被有效阻止：**(2022/08/08)**

- 在**19萬4,400**台端點上，阻止了**7,440**萬次嘗試掃描**Web**服務器的漏洞。
- 在**38萬1,600**台端點上，阻止了**3,750**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬1,200**台**Windows**伺服主機上，阻止了**1,900**萬次攻擊。
- 在**14萬3,300**端點上，阻止了**810**萬次嘗試掃描伺服器漏洞。
- 在**6萬8,600**台端點上，阻止了**330**萬次嘗試掃描在**CMS**漏洞。
- 在**10萬6,500**台端點上，阻止了**310**萬次嘗試利用的應用程式漏洞。
- 在**29萬4,400**台端點上，阻止了**670**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6萬**台端點上，阻止了**390**萬次加密貨幣挖礦攻擊。
- 在**40萬6,000**台端點上，阻止了**560**萬次向惡意軟體**C&C**連線的嘗試。
- 在**5,600**台端點上，阻止了**17萬2,400**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。

## 2022/08/11

## 觀察到 VileRAT 的後門活動

VileRAT 是一個具有資訊竊取功能的後門，自 2020 年以來，一個名為 DeathStalker 組織一直在針對各行各業的公司使用它來發動攻擊，特別是從事與外匯和加密貨幣相關的公司。威脅者最喜歡的感染媒介是假冒知名公司的魚叉式電子郵件。如果受害者回覆這些電子郵件並參與對話，則攻擊者將在某個時候回覆一個谷歌磁碟鏈接，該鏈接將下載惡意 LNK 檔案。在某些情況下，可能會使用惡意 Word 檔來觸發攻擊鏈。一旦攻擊鏈被觸發，一個名為 VileDropper 注入程式將注入一個名為 VileLoader 載入程式，該載入程式將呼叫最終有效籌載--VileRAT。

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.Efplir!gen1
- Trojan.Gen.2
- Trojan.Gen.NPE
- Trojan horse
- Suspicious: Reputation
- W97M.Downloader

**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: Malicious Domain Request 63
- Web Attack: Webpulse Bad Reputation Domain Request

**基於機器學習的防禦技術：**

- Heur.AdvML.B

---

## 2022/08/11

## 在韓國流行的 GwisinLocker 勒索軟體

GwisinLocker 顯然是以韓國民間傳說中的一種精神或鬼魂命名，稱為“Gwisin”(귀신)。該勒索軟體於 7 月首次被發現，其主要目標是韓國工業和製藥公司。作為 Linux 勒索軟體變種，GwisinLocker 在其活動中採用雙重勒索方法。生成的勒索軟體說明文件 (!!!_HOW_TO_UNLOCK_MCRGNX_FILES_!!!.TXT) 包括聯繫資訊以及從公司內部竊取的數據和知識產權列表。

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：**

- Ransom.GwisinLocker
- Trojan Horse
- WS.Malware.2

## 2022/08/11
## Orchard (*果園)：全新的殭屍網路

觀察到一個名為 Orchard 的全新殭屍網路，其使用比特幣發明者：中本聰 (Satoshi Nakamoto) 的資訊來建立惡意網域，以隱藏其命令和控制 (C&C) 基礎設施。自 2021 年 2 月以來，該殭屍網路至少經歷 3 次修訂，其主要目的是將額外的有效籌載部署到受害者機器上並執行從 C&C 伺服器接收到的命令。殭屍網路其他功能包括上傳設備和用戶資訊以及感染 USB 儲存設備，以幫助傳播惡意軟體。

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.Gen.MBT

**基於機器學習的防禦技術：**

- Heur.AdvML.B
- 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。

---

## 2022/08/11
## CopperStealer 竊密程式，助長加密貨幣盜竊的氾濫

在過去幾個月，CopperStealer 竊密程式越來越流行，據報導，它的營運商一直持續強化它的功能。在最近透過瀏覽網頁的順道式下載 (drive-by-download) 攻擊行動中，已經看到該威脅透過惡意瀏覽器外掛程式來竊取加密貨幣交換網站使用的受害者 API 密鑰。如果成功，威脅者會替換成攻擊者的加密貨幣錢包來竊取它們。

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.Di!Gen1
- SONAR.Heur.Dropper
- SONAR.Rarsfx!Pua

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Suspicious: Reputation
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Reputation.1

**基於機器學習的防禦技術：**

- Heur.AdvML.C

## 2022/08/11

## 死灰復燃的 Onyx 勒索軟體

Onyx 是另一種勒索軟體，在無聲無息兩個月後，近期又在真實網路上被觀察到。這個基於 .NET 威脅背後的威脅者參照 Chaos 勒索軟體來開發它，一樣採用雙重勒索戰術。截至今天，它主要針對美國的公司，且告中假設 Onyx 有可能由 Conti 的關聯附屬公司營運，或者至少一個受害者在 Conti 和 Onyx 的洩密網站上被報導後與他們合作。

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.SuspDrop!gen1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.Sorry

---

## 2022/08/11

## 還是很多人從來不修補漏洞，SmokeLoader 單靠陳年老漏洞，依舊屹立不搖

SmokeLoader 惡意載入程式已經存在好幾年，並且仍然潛伏在威脅領域。多年來，他們的作案手法並沒有太大變化，直到今天，我們仍然看到舊的 Microsoft Office 漏洞被利用為作惡意電子郵件的感染媒介。該惡意軟體主要用作載入程序，但也被視為具有資訊竊取功能的機器人。自從首次觀察到它以來，已經載入許多惡意軟體系列。

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：**

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Exp.CVE-2017-0199!g4
- Exp.CVE-2017-11882!g3
- Trojan.Gen.NPE
- Trojan Horse
- Trojan.Mdropper

## 2022/08/10

## BlueSky (*藍天) 勒索軟體

BlueSky 是一個普通的勒索軟體集團，最近出現在已如過江之鯽的勒索軟體領域。在加密方面，他們的勒索軟體與 Conti 和 Babuk 等其他軟體有一些相似之處。根據多份報告，該勒索軟體似乎是透過瀏覽網頁的順道下載攻擊 (Drive-by-download) 所散佈發，目前該組織並未使用雙重勒索戰術 (先竊取再加密，勒索不成則公開竊取的資訊)。

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：

**基於行為偵測技術(Snoar)的防護：**

- AGR.Terminate!g2
- SONAR.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g12

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.Conti!gm1

**基於機器學習的防禦技術：**

- Heur.AdvML.B

---

## 2022/08/10

## Android 平台上的間諜軟體 -- Dracarys

Fireworm (又名 Bitter) 是一個進階持續威脅 (APT) 組織，多年來主要的活動範圍在南亞，現在也開展間諜行動。最近，他們另一項行動被曝光，因為在相似的網路釣魚網站中發現偽裝成 Android 平台上知名的訊息應用 APP。如果受害者無安全意識被這些虛假網站和 App 所誘騙，他們最終會安裝一個名為 Dracarys 的間諜軟體。

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：

**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

**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。

## 2022/08/09
## Redline 竊密程式藉由資本利得稅和加密貨幣等社交工程在澳洲大爆發

Redline 竊密程式在過去的幾個月聲名大噪，因為它一直是全球駭客集團或個人用於竊取世界各地中大型企業重要資訊的首選竊密程式。他們後續要做的事情從敲詐受害者到出售他們的資料和進入地下市場。賽門鐵克會定期觀察針對特定公司的非大型攻擊行動。最近行動中，一名威脅者試圖透過以資本利得稅和加密貨幣相關主題的惡意電子郵件入侵澳洲的金融單位，建議澳洲政府進行重大法令修正。這些電子郵件包含一個 Zip 檔，其中有偽裝成 PDF 報告的 Redline 竊取程式二進位檔案 (檔名：updated KYC T&Cs-pdf.exe)。

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

---

## 2022/08/09
## Lokibot 襲擊拉丁美洲，以 IMG 和 LHZ 格式的檔案進行散佈

Lokibot 存在的時間已久並在全球盛行，大多數人現在對 Lokibot 的危害已經習以為常。賽門鐵克最近觀察到一項主要針對拉丁美洲各行各業的攻擊行動，之前也曾在西班牙和葡萄牙出現過。有好幾位威脅者利用一種經典的銀行轉帳社交工程戰術，據稱該戰鎖定墨西哥一家知名銀行。這些電子郵件夾帶兩個檔案 (IMG 和 LHZ)，兩者都包含 Lokibot 二進製檔案。該惡意軟體能夠從數百個應用程式中竊取憑證，包括瀏覽器、FTP 用戶端、電子郵件用戶端、SSH 用戶端和密碼管理軟體。

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：

**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 Horse

**基於機器學習的防禦技術：**

- Heur.AdvML.B

## 2022/08/09

### 全球都有 Remcos 攻擊行動，日本更是被鎖定的重點

Remcos 已存在多年，是一種精密且熱門的遠端存取木馬 (RAT)。雖然感染媒介沒太大變化，主要透過惡意電子郵件在目標和非目標行動中傳播，但已經看到駭客集團和個人在他們的攻擊鏈中輪換不同的作案手法。最近一項攻擊行動聲明大噪，因為該威脅者針對全球公司，尤其是日本。他們似乎一直在使用仍然相對有效常用且老套的社交工程手法 (主旨：見積のリクエスト：RFQ-20220809024012220JP)。這些電子郵件包含一個圖像附件，其中有 Remcos 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：**

- Trojan Horse

**基於機器學習的防禦技術：**

- Heur.AdvML.C

---

## 2022/08/07

### 假的 Windows 更新程式伴隨著 Gomorrah 竊密程式

Gomorrah 是一個針對密碼和加密貨幣錢包的普通竊密程式。這種惡意軟體在 2020 年初首次出現並在地下銷售，且被多個團體和個人使用。截至今天，賽門鐵克繼續追蹤其活動，儘管與其他惡名昭彰的竊密程式相比，其流行程度很低。最近觀察到一個假的 windows更新程式，藉由瀏覽網頁時順道下載攻擊行動，夾帶 Gomorrah 竊密程式。

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 Horse

**基於機器學習的防禦技術：**

- Heur.AdvML.C

## 2022/08/07

## 抖音用戶 (TikTok) 遭受加密貨幣剪貼簿竊密器 (Clipper) 攻擊

這幾年，抖音 (TikTok) 短片發布和社交媒體服務已經大受歡迎。截至今天，它是全世界青少年和年輕人的主要使用軟體。眾所周知，這群人也大量接觸加密貨幣，理所當然也成為那些心懷不軌的人覬覦的目標。賽門鐵克最近觀察到一個藉由瀏覽網頁所發動的順道下載 (drive-by-download) 攻擊活動，其中一個威脅者劫持 TikTok 用戶，希望透過機器人瀏覽等捷徑提高他們的瀏覽量。用戶幾乎不知道，如果騙成功，他們實際上會安裝一個加密貨幣剪貼簿竊密器，其主要目的是將受害者的加密貨幣錢包位址與惡意軟體威脅者所擁有的位址進行交換。

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
- WS.Malware.1

**基於機器學習的防禦技術：**

- Heur.AdvML.C

## 2022/08/05

## 最近的攻擊行動利用 Dark Utilities C2aaS (C&C 即服務) 平臺

據報導，多個威脅組織利用一個新發佈 Dark Utilities 的 C2aaS (C&C 即服務)平臺。該平臺將指揮和控制中心 (C&C) 基礎設施作為一項服務提供給網路犯罪分子。它還在星際檔案系統 (IPFS) 內託管惡意的有效籌載--這是一個用於儲存資料分散式點對點網路系統的檔案共享系統，以便儲存和共享檔案、網站、應用程式。最近在網路上的一些惡意軟體散佈行動，被觀察到使用 Dark Utilities 進行 C&C 通信--其中少數偏重於遠端存取、DDoS 和加密挖礦。

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
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

**基於機器學習的防禦技術：**

- 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。