
# 保安資訊--本周(台灣時間2022/06/17)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 110 萬個受保護端點上總共阻止了1.967億次攻擊。這些攻擊中有 95% 在感染階段前就被有效阻止：**(2022/06/13)**

- 在**20萬9,100**台端點上，阻止了**9,550萬次**嘗試掃描**Web**服務器的漏洞。
- 在**44萬1,000**台端點上，阻止了**4,010萬次**嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**7萬5,700**台**Windows**伺服主機上，阻止了**2,040萬次**攻擊。
- 在**15萬100**端點上，阻止了**910萬次**嘗試掃描伺服器漏洞。
- 在**7萬8,700**台端點上，阻止了**390萬次**嘗試掃描在**CMS**漏洞。
- 在**11萬3,500**台端點上，阻止了**370萬次**嘗試利用的應用程式漏洞。
- 在**32萬9,300**台端點上，阻止了**950萬次**試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**800**台端點上，阻止了**390萬次**加密貨幣挖礦攻擊。
- 在**10萬9,200**台端點上，阻止了**600萬次**向惡意軟體**C&C**連線的嘗試。
- 在**7,200**台端點上，阻止了**28萬8,100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。

## 2022/06/16

## 被稱為 "MaliBot" 的新型 Android (*安卓) 行動惡意軟體變種

MaliBot 是一個 Android 平台竊密木馬的全新變種，被發現針對西班牙和義大利用戶的網路銀行和加密貨幣錢包。

MaliBot 一些主要特徵包括：

- 將自己偽裝成一個名為 "Mining X" 或 "The CryptoApp" 的加密貨幣挖礦 App，偶爾也會偽裝成如 "MySocialSecurity" 和 "Chrome" 等假冒 App。
- 主要破壞力是竊取金融資訊、憑證、加密貨幣錢包和個人資料 (PII)，還針對義大利和西班牙的金融機構。
- 能夠竊取密碼和繞過多因子認證機制 (2FA/MFA)。
- 包括具有遠端控制使用 VNC 伺服器的受感染設備能力。

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.Gen.2
- WS.Malware.1
- WS.Malware.2

**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.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。

---

## 2022/06/16

## Cobalt Strike 和 XMRig 透過利用一個舊的 CVE-2019-18935 Telerik 使用者介面 (UI) 漏洞進行傳播

根據報告，在最近的惡意軟體散佈行動中觀察到針對三年前就已經存在的 Telerik 使用者介面 (UI) 漏洞之遠端程式碼執行 (CVE-2019-18935) 漏洞刺探攻擊。攻擊者一直鎖定脆弱的 Web 伺服器，在努力提供 Cobalt Strike 信標的同時，也會啟動 PowerShell 腳本，最終能夠交付 XMRig 加密程式的有效酬載。目前的行動與被稱為 Blue Mockingbird (*藍色知更鳥) 威脅組織的一些過往行動有某些相似之處，該組織早在 2020 年就已經在利用相同的 Telerik UI 漏洞，針對微軟 IIS 伺服器發動攻擊。

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：

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.Cobalt!gm5
- Meterpreter
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1

**基於機器學習的防禦技術：**

- 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: Telerik UI CVE-2019-18935
- Web Attack: Telerik UI CVE-2019-18935 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。

---

## 2022/06/16

## 用 Nim 撰寫 IceXLoader 新版本

IceXLoader 是一種商業惡意軟體，用於在受感染的機器上下載和部署額外的惡意軟體，通常在攻擊鏈的第二或第三階段。該惡意軟體的一個新版本被發現採用 Nim 撰寫，Nim 作為威脅者使用的語言相對較新。

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 Horse
- WS.Malware.1
- WS.Malware.2

**基於行為偵測技術(Snoar)的防護：**

- SONAR.SuspBeh!gen66
- SONAR.SuspDataRun
- SONAR.SuspDrop!gen1

**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已於第一時間收錄於不安全分類列表中。

## 2022/06/16

### 持續在真實網路環境發現大量利用代號：CVE-2021-26086 的 Jira Atlassian 漏洞刺探攻擊

在過去幾週裡，賽門鐵克的網路保護技術--入侵防禦系統 (IPS) 根據威脅態勢監測發現掃描結果，這些掃描結果顯示對一個稍早且已經釋出修補程式的 Jira Atlassian 漏洞利用有上升趨勢。CVE-2021-26086 是 Jira 軟體伺服器中的一個路徑遍歷 (Path traversal) 和檔案讀取權限的漏洞。該漏洞允許遠端攻擊者讀取和竊取檔案和資訊。攻擊者的目標是竊取包含機敏資訊的檔案，例如：日誌資料和配置設置。這些機敏資訊隨後可被攻擊者用於更進一步的利用。

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: Atlassian Jira Server File Disclosure CVE-2021-26086

---

## 2022/06/15

### 發現 Syslogk---一個 Linux 平台上全新的 rootkit

一個被稱為 Syslogk 的 Linux 平台上全新 rootkit 已經在真實環境到處亂竄。根據最近報告，Syslogk 是基於一個被稱為 Adore-Ng 舊版開放原始碼的 rootkit，並且似乎正在積極開發中。該 rootkit 具有隱藏被感染電腦上含有惡意檔案目錄以及惡意網路流量的功能。Syslogk 還具有隱藏惡意有效籌載的能力--在這種情況下應該是 Rekoobe 惡意軟體家族的後門。

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：**

- Backdoor.Trojan
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- WS.Malware.2

## 2022/06/15

### 微軟 6 月更新修補發佈的覆蓋範圍詳細資訊

6 月 14 日微軟發佈定期每月更新。對應 6 月份更新發佈，微軟已經解決 56 個漏洞。解決漏洞之一但沒有明確列出是最近披露的 Follina 漏洞，該漏洞已被確認為遭到積極刺探攻擊利用。

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：**

- Exp.CVE-2022-30190

**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：

- Exp.CVE-2022-30190

---

## 2022/06/14

## PureCrypter 載入程式

PureCrypter 是一個載入程式，它為各種組織和個體提供在其攻擊鏈中增加另一層次的規避能力，有利於部署 (透過植入) 其有效籌載。自 2021 年 3 月左右首次在地下市場上宣傳和銷售以來，迅速遍地開花，並被觀察到部署各種遠端存取木馬和竊密程式。

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.Gen.2
- Trojan.Gen.MBT
- Trojan Horse

---

## 2022/06/14

## Gallium (*伽利略)進階威脅組織 (APT) 使用 PingPull 遠端存取木馬 (RAT) 發動攻擊

一個新的遠端存取木馬 (RAT) 被稱為 PingPull，已被 Gallium APT 組織在進行的攻擊中使用。攻擊者一直在針對歐洲、東南亞和非洲的電信部門、金融機構和政府組織。PingPull 使遠端威脅者能夠利用 reverse shell 來接管被攻擊電腦的控制權，並賦予執行任意命令的能力。根據不同的變種，PingPull RAT 可能使用不同的協議進行 C&C 伺服器通信，這些協議包括 TCP、HTTPS 和 ICMP。

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

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

**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 674

**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。

---

## 2022/06/14

## Hydra 行動惡意軟體透過假的手機檔案管理應用程式傳播

一個傳播 Hydra 移動惡意軟體的新行動已經被發現，其中的惡意應用程式已經出現在 Google Play 商店中。該惡意軟體偽裝成一個手機檔案管理應用程式，自發佈以來被下載超過 10,000 次。Hydra 是自 2019 年以來在網路威脅生態中看到的一個行動銀行木馬變種。該惡意軟體的功能允許它竊取 cookie、簡訊內容、電話簿的連絡人、OTP或設備鎖定密碼等。

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：

**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

**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。

---

## 2022/06/13

## 編號：CVE-2022-26134 對應 Atlassian 公司的 Confluence 漏洞在真實環境被大量濫用

據報導，編號：CVE-2022-26134 對應 Atlassian 公司的 Confluence漏洞 (註：Confluence 為模組化的知識管理平台)，被一些威脅者在真實環境大量濫用，以傳播僵屍網路或惡意勒索軟體。這個遠端程式碼執行 (RCE) 漏洞與物件圖形導向語言 (OGNL) 的注入有關，允許未經認證的使用者有機會在被入侵的系統上執行任意程式碼。目前在濫用這個漏洞的攻擊主要有 Kinsing 和Mirai 殭屍網路等惡意軟體家族，以及 AvosLocker 和 Cerber2021 勒索軟體變種。

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：**

- Downloader
- Ransom.Cerber
- Trojan Horse
- 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: Atlassian OGNL Injection CVE-2022-26134
- Web Attack: Malicious Java Payload Upload 5

**基於安全強化政策(適用於使用DCS)：**

使用 DCS 預設強化政策就能輕鬆對 Confluence 伺服器實例進行保護。

**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。

---

## 2022/06/13

## HelloXD勒索軟體

HelloXD 是一個早在 2021 年底前後被發現的勒索軟體變種。該惡意軟體顯示出與洩露的 Babuk 惡意軟體變種有某些程式碼重疊。根據一份最新的報告，HelloXD 被認為是一個被稱為 x4k 的威脅者所為。一些被發現的勒索軟體樣本還在被感染的機器上部署一個被稱為 MicroBackdoor 的輔助開放原始碼後門。這個後門允許攻擊者經由執行遠端命令和上傳／下載檔案等方式進一步入侵系統。

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(Snoar)的防護：**

- AGR.Terminate!g2
- SONAR.RansomGen!gen2
- SONAR.Ransomware!g1
- SONAR.SuspDataRun
- SONAR.SuspLaunch!g18

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.Cobalt!gen9
- Backdoor.Cobalt!gm5

- Downloader
- Meterpreter
- Packed.Generic.347
- Ransom.Helloxd
- 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

**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。

---

## 2022/06/10

## Lyceum 進階持續威脅 (APT) 組織使用 .NET 的 DNS 後門

一個新 .NET 的客製化 DNS 後門，最近被用於 Lyceum 進階持續威脅 (APT) 組織發起的惡意行動。該後門使用的程式碼源自一個名為 dig.net 開放原始碼的 DNS 名稱遞迴解析工具 (Resolver)。該惡意軟體利用 DNS 劫持技術，採用 DNS 協議與攻擊者的 C2 伺服器進行通信。該後門還具有上傳／下載檔案以及在被入侵系統上執行遠端命令的功能。

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：

**檔案型(基於回應式樣本的病毒定義檔)防護：**

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

**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已於第一時間收錄於不安全分類列表中。

---

## 2022/06/10

## Symbiote -- 一種針對 Linux 的新型惡意軟體

一種全新針對 Linux 平臺的惡意軟體，被稱為 Symbiote，已在網路上到處流竄。Symbiote 沒有使用獨立的惡意可執行檔，而是以共用物件（SO）程式庫的形式載入到被攻擊機器的所有執行程序中。該惡意軟體允許攻擊者遠端存取電腦，並有能力收集用戶憑證等。與上個月剛剛發

現的 BPFDoor 惡意軟體類似，Symbiote 利用 Berkeley Packet Filter（BPF）封包過濾元件來隱藏其在受感染主機上攻擊流量。

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.NPE
- 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已於第一時間收錄於不安全分類列表中。

---

## 2022/06/10

## 要求遊戲幣 (R幣-Robux) 當贖金的全新勒索軟體：WannaFriendMe

Roblox 是近年熱門的元宇宙概念多人線上遊戲開發平臺，允許玩家可以在這個空間內創作自己或他人開發的遊戲，並透過出售體驗證 (Game Passes) 來獲得特殊的遊戲優惠，進而實現盈利。體驗證 (Game Passes) 只能用專屬遊戲幣 (R幣--Robux) 購買。

被稱為 WannaFriendMe 的勒索軟體似乎在模仿 Ryuk 勒索軟體，因為它在受感染的檔案上附加 .ryuk 副檔名，但研究顯示，該變種更可能是 Chaos 勒索軟體。比較特殊的地方是，WannaFriendMe 不要求常見的加密貨幣，而是要求受害者使用體驗證 (Game Passes) 來支付贖金以獲取解密金鑰。

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.Chaos
- WS.Malware.1

**基於機器學習的防禦技術：**

- Heur.AdvML.B