
# 保安資訊--本周(台灣時間2023/07/14)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 68 萬 8,200 台受保護端點上總共阻止了 8,210 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/07/10)**

- 在**13萬9,300**台端點上，阻止了**3,250**萬次嘗試掃描**Web**服務器的漏洞。
- 在**24萬5,300**台端點上，阻止了**1,810**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬2,600**台**Windows**伺服主機上，阻止了**1,330**萬次攻擊。
- 在**9萬4,200**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,800**台端點上，阻止了**82萬1,100**次嘗試掃描在**CMS**漏洞。
- 在**7萬2,200**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**22萬3,900**台端點上，阻止了**540**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**3,100**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**14萬1,000**台端點上，阻止了**930**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**8萬2,900**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。

## 2023/07/13

## Proton(*質子)勒索軟體

在駭客圈要闖出名號，總要有幾把刷子。在過去的幾個月裡，Proton(*質子)勒索軟體算是異軍突起的後起之秀。根據贖金支付說明，該駭客集團被稱為 Proton，似乎並未採用雙重勒索伎倆。當電腦被成功加密後，檔案會被新增 .proton 或 .Kigatsu 的副檔名。贖金支付說明中沒有具體說明贖金金額。截至目前，這只是一個常見問題解答，為受害者提供編號 ID，並包括歹徒的 Telegram 和電子郵件聯繫人。

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

**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

---

## 2023/07/13

## Linux平台上的BPFDoor惡意後門程式～更版了

BPFDoor 是在 Linux 和 Solaris 平台相當活耀的惡意後門程式，最初於 2021 年發現。該惡意軟體利用 Berkeley Packet Filter (BPF) 封包監聽工具來監控網路流量，並僅在現有開放埠號上傳遞封包，以繞過防火牆規則和網路保護。BPFDoor 的最新版本發揮新版 BPF 的功能，證明該後門仍在由其背後的威脅組織積極開發中。

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：

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Backdoor.Trojan
- Linux.BPFDoor
- Linux.Lightaidra
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

## 2023/07/13

## 不補漏洞被駭有理～最新的Lokibot攻擊行動還是針對未修補的老舊漏洞

最近在開採利用兩個相當老舊的 MS 遠端程式碼執行 (RCE) 漏洞（CVE-2021-40444 和 CVE-2022-30190）的攻擊行動中觀察到 Lokibot 惡意軟體。攻擊者一直在 MS Office 文件中嵌入惡意巨集，一旦執行，就會導致感染最終有效籌載。Lokibot 惡意軟體在威脅領域已存在多年，已知主要透過惡意垃圾郵件傳播並用於竊取資訊。

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(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：**

- Infostealer.Lokibot
- Trojan Horse
- Trojan.Gen.2
- Trojan.Malscript
- W32.IRCBot.NG
- W97M.Downloader
- WS.Malware.2

**基於機器學習的防禦技術：**

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

**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: Microsoft MSHTML RCE CVE-2021-40444
- Web Attack: MSDT Remote Code Execution CVE-2022-30190
- 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。

## 2023/07/12

## 小心新型USB隨身碟病毒：SOGU和SNOWYDRIVE惡意軟體

研究人員報告指出，這些攻擊行動的重點是利用 USB 隨身碟作為其初始的感染管道。在最初始的入侵後，SOGU 目標將被誘使啟動一個包含惡意 DLL 載入程式的合法檔案。透過 SNOWYDRIVE，目標受害者將被引誘點擊偽裝成合法檔案的惡意軟體。

這些惡意軟體的主要目標是竊取資料，並且它們支持多種命令，包括檔案傳輸、檔案執行、遠端桌面、螢幕截圖、反向 shell 和鍵盤側錄。

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：**

- Heur.AdvML.A!300
- 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。

---

## 2023/07/12

## 最新公告的Office和Windows HTML遠端程式碼執行(RCE)漏洞(CVE-2023-36884)已被開採利用發動目標式攻擊

影響 Microsoft Windows 和 Office 產品的零日漏洞 (CVE-2023-36884) 正在被歹徒廣泛開採利用。迄今為止，該漏洞已被用於針對歐洲和北美政府和國防部門組織的高度針對性的攻擊。該漏洞由微軟昨天（7月11日）披露，稱攻擊者可以建立特製的 Microsoft Office 文件，從而能夠在目標電腦上遠端執行惡意程式碼。為了成功利用該漏洞，受害者需要打開惡意文件。目前尚未發布針對該漏洞的修補。

在我們的部落格中閱讀更多內容：攻擊者利用未修補的 Windows 零日漏洞。

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：

**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.Mdropper
- 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：

- 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。

---

## 2023/07/11

## 『利而誘之，亂而取之。』～Chaos勒索軟體誘騙Roblox玩家

在遊戲世界中追求輕鬆獲勝，長期以來使遊戲玩家容易成為網路犯罪分子覬覦的目標。這是因為作弊工具的散布和託管方式的本質創造一個駭客駕輕就能得逞的環境。此外，由於玩家之間固有的信任，玩家經常互相共享和交換檔案、模組或作弊程式，從而培養一種友誼和協作感。

作弊工具通常通過遊戲社群內的各種管道共享。其中包括地下論壇、不起眼的網站、私人聊天室、檔案共享平台，甚至社交媒體。駭客組織與個體戶每天都會滲透到這些管道，誘使遊戲玩家下載偽裝成作弊工具的惡意軟體（竊密程式、遠端存取木馬、勒索軟體、挖礦程式、加密貨幣錢包剪貼簿竊密器 (Clipper) 等），從而允許他們未經授權存取遊戲玩家的系統、個人資訊，或遊戲帳戶。

在最近的一個例子中，賽門鐵克發現到一名歹徒使用作弊軟體引誘 Roblox 玩家。然而，玩家並沒有獲得預期的功效，反而發現自己電腦上的所有檔案被 Chaos 索軟體給加密了。隨後，歹徒索價等同 200 美元的比特幣贖金，才能提供解密。

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.SuspDrop!gen1

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.Sorry

**基於機器學習的防禦技術：**

- Heur.AdvML.B

## 2023/07/10

## 防護亮點：Play勒索軟體

Play 勒索軟體 (也稱為 PlayCrypt) 於 2022 年中左右首次出現，是當今威脅領域最活躍的勒索軟體之一，與 LockBit、Mallox、Clop 等其他惡名昭彰的勒索軟體家族旗鼓相當。該駭客集團已駭入超過 25 名受害者，目標包括各種規模的不同行業等公共與私人組織。與惡名昭彰的同行一樣，該駭客集團因採用雙重勒索伎倆而聞名，受害者將遭到威迫，如果不支付贖金，他們的資料將被出售。


就感染途徑而言，Play 勒索軟體背後的歹徒一直在開採利用已知的漏洞（ProxyNotShell 就是一個例子），並以從其他專門販售存取權限的駭客集團所購得的登入憑證來進行入侵。攻擊者還使用各種駭客工具（例如：Cobalt Strike、MimiKatz、Empire 和遠端存取木馬 (RAT)）進行橫向移動和常駐。Play 勒索軟體一旦安裝在系統上，就會加密所有檔案並冠上 .PLAY 的副檔名，並建立檔名為『ReadMe.txt』的贖金支付說明。眾所周知，贖金支付說明內容很短，通常只包含『Play』一詞以及歹徒的洋蔥加密網站的鏈接或用於聯繫他們的電子郵件地址。

賽門鐵克針對 Play 勒索軟體，提供完整的零時差保護，具體說明如下：

**基於行為偵測技術(SONAR)的防護：**

- SONAR.RansomPlay!gen1
- SONAR.RansomPlay!gen2
- SONAR.RansomPlay!gen3

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Ransom.PlayCrypt
- Ransom.PlayCrypt!g1
- Ransom.PlayCrypt!g2

**基於機器學習的防禦技術：**

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

**基於安全強化政策(適用於使用DCS)：**

只要有安裝 Symantec Data Center Security 就能套用預設的安全強化政策來提供針對未知威脅

的零時差攻擊，當然預設強化安全政策就能偵測到以前從未見過的 Play 勒索軟體變種和行為。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

欲瞭解更多有關於賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲瞭解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
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。

---

## 2023/07/10

## Snatch勒索軟體依然活耀

Snatch 是一個勒索軟體家族，至少從 2019 年起就出現在威脅領域中。該惡意軟體至今依然活耀，並定期出現新變種。眾所周知，Snatch 背後的駭客集團採用雙重勒索伎倆，不僅對使用者檔案進行加密，還竊取資料，並脅迫如果不支付贖金將公開遭竊的資料。被該勒索軟體加密的檔案會被新增隨機的附檔名。最近發現該勒索軟體慣用的副檔名實例包括：.hgjzitlxe、.tcvjuo、.tnwkgbvl、.qxtfkslrf、.zuiooseft。

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.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g28

**檔案型(基於回應式樣本的病毒定義檔)防護：**

- Downloader
- Ransom.Snatch
- Ransom.Snatch!g1
- Ransom.Snatch!g2
- Ransom.Snatch!gm
- Trojan.Gen.2
- Trojan.Gen.MBT

**基於機器學習的防禦技術：**

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

## 2023/07/10

## TUGA勒索軟體

TUGA 是最近在真實網路情境所發現到的另一種標準型勒索軟體。該勒索軟體會加密使用者的檔案並附加 .TUGA 的副檔名。附帶的贖金支付說明檔會將受害者引導向 Telegram 頻道與歹徒聯繫。TUGA 勒索軟體具有刪除遭駭入系統上的還原點以及收集系統資訊的功能。最近得逞的勒索軟體背後的歹徒索價 1,000 美元的贖金以換取解密密鑰。

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(SONAR)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：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.B
- 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: Trojan.Backdoor Activity 634

---

## 2023/07/07

## ARCrypter(又名ChileLocker)勒索軟體釋出更強版本

ARCrypter（又名ChileLocker）勒索軟體早在去年就出現，主要針對智利政府機構的攻擊。從那時起，這個勒索軟體背後的歹徒擴大他們的惡意活動，並開始針對世界各地的組織。目前，ARCrypter 有支援 Windows 和 Linux 平臺的版本。最近的變種會加密用戶檔案，並將 .crYpt 副檔名附加到被加密檔。它也有能力停用與安全軟體或備份解決方案有關的程序和服務。這個惡意軟體背後的歹徒者似乎正在為他們的每個受害者建立在 TOR 網路上的各別專用聊天網站。

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.RansomChill!g1
- SONAR.SuspBeh!gen678

**檔案型(基於回應式樣本的病毒定義檔)防護：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.B
- Heur.AdvML.C

---

## 2023/07/07

## 與Truebot惡意軟體有關的惡意活動明顯增加

根據最新的美國網路安全暨基礎設施安全局 (CISA) 公告，Truebot 惡意軟體的全新變種最近在針對美國和加拿大的組織的網路攻擊行動中發現其已經被駭客開始利用。據瞭解，TrueBot 主要透過釣魚郵件傳播，但現在攻擊者也利用 CVE-2022-31199 的漏洞來傳遞該惡意軟體，這是 Netwrix Auditor 軟體的一個遠端程式碼執行（RCE）漏洞，允許未經授權的攻擊者以 SYSTEM 用戶的權限執行惡意程式碼。Truebot 殭屍網路過去曾被與 Cl0p 勒索軟體有關的網路犯罪歹徒廣泛使用。

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：

**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：**

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

**基於機器學習的防禦技術：**

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.B
- 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：

- 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。

---

## 2023/07/07

## Blank Grabber(*空白抓取器)惡意竊密程式

Blank Grabber 是一種惡意竊密程式，至少從 2022 年起就在駭客圈出現。該惡意軟體具有竊取機密使用者資料的功能，包括憑證、cookies、加密貨幣錢包、流覽器內存儲的資料、Discord 帳號的 Token 和其他。Blank Grabber 利用 Discord 和 Telegram webhooks 進行指揮和控制 (C&C) 通訊以及資料竊取滲透。

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：**

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

**基於機器學習的防禦技術：**

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

---

## 2023/07/07

## Agent Tesla(*特斯拉特工)惡意竊密程式正在危害印尼

Agent Tesla 是最常見的惡意竊密程式之一，多年來在駭客圈一直有很高的排名與影響力。它被全球許多駭客組織與個人所使用，也已在不同語系的國家發動攻擊行動。賽門鐵克觀察到一個針對印尼公司的全新網路攻擊行動，特別是在汽車、金融、油脂化學品、電子和食品行業。

此一行動背後的歹徒並沒有採用複雜的社交工程伎倆。相反，他們依靠一種常見的方法--稅務發票。惡意電子郵件（主題：Copy Faktur Pajak Masa Juni - July 2023）被發送，並附上一個 .RAR 壓縮附件案。如果使用者被欺騙，他們將執行內含於附件檔中 Agent Tesla 惡意程式檔案。

Agent Tesla惡意軟體的影響可能是巨大，從經濟損失和身份盜竊到敏感資訊的外洩和正常系統功能的破壞。

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：**

- Scr.Malcode!gdn32

**基於機器學習的防禦技術：**

- Heur.AdvML.B!200