保安資訊--本周(台灣時間2023/08/11)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 66 萬 3,700 台受保護端點上總共阻止了 7,480 萬次攻擊。這些攻擊中有 92.9% 在感染階段前就被有效阻止：**(2023/08/07)**

- 在**12萬3,000**台端點上，阻止了**2,660**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**20萬8,800**台端點上，阻止了**1,670**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬900**台**Windows**伺服主機上，阻止了**1,330**萬次攻擊。
- 在**7萬6,300**台端點上，阻止了**240**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,500**台端點上，阻止了**92萬2,900**次嘗試掃描在**CMS**漏洞。
- 在**5萬5,700**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**23萬6,600**台端點上，阻止了**570**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,300**台端點上，阻止了**170**萬次加密貨幣挖礦攻擊。
- 在**12萬5,700**台端點上，阻止了**940**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,100**台端點上，阻止了**9萬2,300**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。

2023/08/10

在真實網路情境觀察到STRRAT遠端存取木馬的新版本：增強對安全軟體的偵測規避能力

已在真實網路情境發現到由 Java 撰寫 STRRAT 遠端存取木馬的最新 1.6 版本。該惡意軟體透過夾帶 .pdf 附件的惡意垃圾郵件進行傳播，該附件會導致 .zip 壓縮檔下載並透過惡意 JavaScript 進行有效籌載傳遞。相較於舊版本，新版的 STRRAT 功能基本上差異不大，原來就具有憑證盜竊、鍵盤側錄、命令執行、控制遭入侵的系統以及下載／安裝額外的任意有效籌載等功能。1.6 新版導入兩種字串混淆技術，增強惡意軟體的檢測規避能力。

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：

- ISB.Dropper!gen12
- ISB.Dropper!gen35
- Trojan Horse
- Trojan.Gen.NPE
- Scr.Malcode!gen
- Scr.Malcode!gen69
- 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: JS.Downloader Activity 34
- System Infected: Trojan.Backdoor Activity 410
- 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。

2023/08/10

假冒SBI等銀行的回饋獎勵APP的Android銀行惡意軟體，在印度造成災難

印度有 65% 的人口是居住在農村地區。印度大多數知名銀行都在擴張並擁有大量農村分支機構。由於方便進行金融交易，網路銀行在印度農村人口中日益受歡迎。然而，隨著網路銀行的興起，這些農村人口現已成為銀行欺詐的主要目標。

過去幾週，我們發現更多針對印度智慧型手機用戶的 Android 銀行惡意軟體偽裝成 SBI 等知名銀行的銀行回饋獎勵 APP。攻擊者可能會使用詐騙／網路釣魚／網路釣魚等各種技倆來引誘受害者安裝偽裝成銀行回饋獎勵 APP 的惡意程式。安裝後，該惡意軟體允許攻擊者竊取簡訊並攔截雙因素身份驗證 (2FA)，可利用該身份驗證來存取機敏資訊，例如：電子郵件帳戶和其他形式的個資，這可能進一步導致後續的錢財損失。

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
- AppRisk:Generisk

2023/08/10

CraxsRAT～全新的安卓手機行動裝置上的遠端存取木馬

在網路世界充斥著許多各式各樣的惡意木馬程式，在安著手機平台更是如此，在網路隨便下載就唾手可得的惡意木馬程式，許多是源於遭破解或洩漏的專業版本的惡意木馬程式，所以其功能、流行程度以及防禦的困難度都達到一定的專業水準。

CraxsRAT 是一種最新的遠端存取木馬，在 Telegram、其他社交網站、網站、軟體開發平台和地下論壇上進行廣告宣傳。它在被破解和洩露後，被大肆公開分享，吸引許多駭客組織及個人的目光，而被利用於更多的活動（攻擊和測試）。

就跟常見的手機行動裝置上的遠端存取木馬一樣，CraxsRAT 具有遠端存取木馬 (RAT)、惡意間諜程式以及竊密程式等功能。

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：

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。

- AppRisk:Generisk

2023/08/10

難怪北韓的飛彈技術突飛猛進～ScarCruft和Lazarus駭客組織與俄羅斯導彈公司的網路入侵事件有關

賽門鐵克獲悉有關俄羅斯飛彈公司遭受網路攻擊的報導，據稱是北韓國家級駭客組織：ScarCruft 所發動。雖然他們不是參與此次網路間諜攻擊行動的唯一參與者，但他們發現一個名為『OpenCarrot』的後門，該後門與另一個更舉世聞名的北韓國家級駭客組織：Lazarus 有關。

截至撰寫本文時，初始存取／入侵初期的方法仍不確定。然而，這些駭客組織因採用多種技術滲透受害者網路而聞名。這些技術包括網路釣魚電子郵件、開採利用企業軟體中的漏洞以及利用被盜的憑證／帳密。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Trojan Horse
- Trojan.Gen.MBT

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

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

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。

2023/08/09

利用Rhysida勒索軟體來發動網路攻擊的活動激增

根據美國衛生與人類服務部（Department of Health & Human Services）的醫療部門網路安全協調中心（Healthcare Sector Cybersecurity Coordination Center，HC3）的最新通報，利用 Rhysida 勒索軟體來發動網路攻擊的活動有所激增。Rhysida 以勒索軟體即服務 (Raas) 的形式出現，早在 5 月份就首次出現在真實網路情境，從那時起就在多起攻擊行動中廣為傳播。Rhysida 背後的攻擊者主要針對教育、醫療保健、政府和製造部門等。眾所周知，傳播 Rhysida 的攻擊利用網路釣魚行動進行初期入侵（Initial Access），並利用滲透測試工具 Cobalt Strike的Beacon 元件，進一步深入感染鏈。該勒索軟體採用多執行緒加密技術，也預先將特定的副檔名／目錄列為加密除外清單，被加密後的檔案將會被冠上 .rhysida 的副檔名。

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.Ransom!gen10
- SONAR.Ransomware!g1
- SONAR.Ransomware!g2
- SONAR.Ransomware!g3

- SONAR.SuspLaunch!g18
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Rhysida
- 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

2023/08/09

SkidMap攻擊記憶體型資料庫Redis伺服器

根據最近的報告，一個被稱為 SkidMap 全新惡意軟體正在積極針對易受攻擊的 Redis 伺服器，這些伺服器是源於開放原始碼，而且 Redis Server 是在記憶體進行所有的操作，所有資料都透過 Key-Value 的方式存放在記憶體，在找尋所需資料透過 Hashmap 的方式取得，所以速度非常快。這種 Linux 平台上的威脅至少自 2019 年以來就一直活躍。最近這一活動背後的歹徒仍在增強其常駐能力和加密貨幣挖礦的能力。當發現開放的 Redis 伺服器時，他們將部署一個惡意 shell，充當惡意 GIF 或 JPEG 的植入程序。此有效籌載隨後將載入 rootkit 和加密貨幣挖礦程式。

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.NPE
- Trojan Horse

2023/08/08

防護亮點：加密貨幣挖礦攻擊不斷

自從比特幣騰空出世以來，加密貨幣挖礦生態就在網路世界佔有一席之地。多年來，隨著數位金融的普及和市場的擴大，加密貨幣挖礦活動也穩步增長。許多個人和組織將加密貨幣挖礦視為一個前景可期的投資機會，利用他們的運算能力來挖掘加密貨幣並期待致富發財。

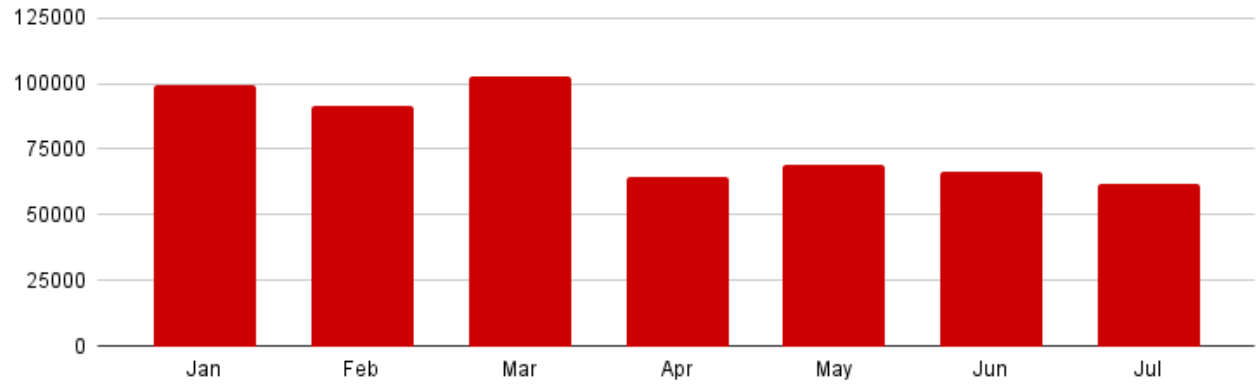
然而，隨著加密貨幣日益主流化，該領域也引起了網路犯罪分子的覬覦。許多消費者和企業不知道的是，他們的電腦和基礎設施成為了加密貨幣挖礦攻擊的主要目標。

這些惡意加密貨幣挖礦程式背後的網路犯罪分子設計了各種複雜的技術來感染系統並秘密入侵運算資源。他們利用惡意電子郵件、遭入侵的網站、偷渡式下載和漏洞開採利用等伎倆來

取得機器的存取權限（以及常駐和橫向移動），隨後神不知鬼不覺地剝削它們的運算資源默默地成為挖礦電腦。

這些網路掏金客總會使用客製化挖礦程式和合法化挖礦程式如吸血鬼般地拼命挖礦。儘管存在對合法挖礦程式的潛在濫用，賽門鐵克長期以來一直對其進行檢測。賽門鐵克每個月都偵測到數萬次以上的挖礦攻擊。

賽門鐵克攔截的挖礦攻擊達數萬次 / 月



這些挖礦攻擊活動的影響甚鉅。對消費者而言，常見的症狀包含電腦運行速度緩慢、電費意外飆升以及設備電池壽命縮短的情況。對於企業來說，後果更為嚴重，包括關鍵運營中斷和潛在的資料外洩。

賽門鐵克提供的單一解決方案內建多層級防護技術，個別技術多能在第一時間就具備**零時差**防護的能力並有明確的定義，僅就不同防護技術說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.Bluwimps*
- SONAR.CoinMiner*
- SONAR.Coinbitminer!g1
- SONAR.GhostMiner!gen1
- SONAR.Gosopad!gen5
- SONAR.Miner*
- SONAR.Suspdrop!g61

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.XMRig!gen1
- Linux.Coinminer
- MSH.Gosopad
- Miner.Bitcoinminer
- Miner.Burst
- Miner.Cpuminer
- Miner.Jswebcoin*

- Miner.Neoscrypt
- Miner.Wasmwebcoin
- Miner.XMRig*
- Miner.Zcash!gen1
- Miner.Zcashminer
- OSX.Coinminer
- OSX.Miner.Coinminer
- PUA.Bitcoinminer
- Trojan.Adylkuzz
- Trojan.Coinbitminer
- Trojan.Coinminer*
- Trojan.Madominer
- Trojan.Minjen*
- Trojan.Shminer
- W32.Coinbitminer
- W32.Mysracoin
- W32.Rarogminer
- W32.Rarogminer!G1
- W32.XiaobaMiner

基於機器學習的防禦技術：

- Heur.AdvML.*

欲深入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。

欲深入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。

欲深入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。

欲深入瞭解賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。

2023/08/04

Rilide竊密惡意程式，釋出新版本

Rilide 竊密程式已知以 Chromium 類型的瀏覽器為目標，例如：Google Chrome、Microsoft Edge、Brave 和 Opera。首次發現幾個月後，據報導，該新版本竊密惡意程式增加支援 Chrome Extension Manifest V3 的能力，使惡意瀏覽器外掛／擴充能夠克服 Google 新擴充功能規範引入的限制，並添加額外的程式碼混淆以逃避檢測。其他新功能包括將被盜資料上傳到 Telegram 頻道的能力，以及每隔一段時間就截取螢幕，並將其傳輸到其專用的 C&C 伺服器。

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
- Trojan.Gen.NPE
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.3

基於機器學習的防禦技術：

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

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。