保安資訊--本周(台灣時間2023/03/17)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 82 萬 2,500 台受保護端點上總共阻止了 9,560 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/03/13)**

- 在**16萬1,700**台端點上，阻止了**4,550**萬次嘗試掃描**Web**服務器的漏洞。
- 在**28萬7,600**台端點上，阻止了**2,070**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬7,300**台**Windows**伺服主機上，阻止了**1,790**萬次攻擊。
- 在**8萬4,900**台端點上，阻止了**310**萬次嘗試掃描伺服器漏洞。
- 在**2萬2,800**台端點上，阻止了**130**萬次嘗試掃描在**CMS**漏洞。
- 在**6萬7,900**台端點上，阻止了**210**萬次嘗試利用的應用程式漏洞。
- 在**27萬6,800**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**5萬1,000**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**14萬4,500**台端點上，阻止了**1,180**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,800**台端點上，阻止了**19萬1,400**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。

2023/03/16

新型殭屍網路又出現：GoBruteforcer--用Golang撰寫的新型殭屍網路

GoBruteforcer 是一種用 Golang 程式語言撰寫的新型殭屍網路。該殭屍網路鎖定以運行 phpMyAdmin、MySQL、FTP 和 Postgres 等服務的網頁伺服主機為目標。一旦掃描到目標有機可趁的主機，殭屍網路將嘗試透過暴力破解密碼攻擊入侵。成功登錄目標系統後，GoBruteforcer 將部署並執行網際網路中繼聊天 (IRC：網際網路中繼聊天) 機器人，該機器人電腦受攻擊者所操控並等待進一步的命令。

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：

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

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。

2023/03/15

利用人性弱點的社交工程：提防與矽谷銀行(SVB)倒閉相關的網路釣魚和欺詐網站

多年來，世界各地的網路罪犯一直在利用銀行作為他們的惡意垃圾郵件和網路釣魚惡意行動的的誘餌。這種社交工程伎倆可能聽起來被過度使用，但它仍然非常有效，當主要銀行倒閉時，網路釣魚跟詐騙就會像像蒼蠅一樣蜂擁而至，你知道嗎？就在矽谷銀行倒閉的消息傳出後，註冊多個似是而非、拼寫錯誤的域名，其中一些被用於網路釣魚攻擊。

某些人總是透過註冊與熱門或經常瀏覽網站的相近網域名稱，例如：輕微拼寫錯誤或順序對調的域名搶註現狀就很多。註冊相似網域名稱的人期望將合法網站的流量重定向到他們自己的網站。他們就可使用這種伎倆來產生廣告收入、銷售仿冒商品，甚至竊取個人資訊。

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：

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)。

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。

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。

2023/03/15

YoroTrooper駭客組織鎖定獨立國協(CIS:Commonwealth of Independent States)

被稱為 YoroTrooper 的新駭客組織在針對獨立國協 (CIS) 國家／地區政府組織的間諜攻擊中被發現。YoroTrooper 駭客組織利用各種自定義和開放原始碼工具、竊密程式和遠端存取木馬(RAT)，例如：Stink Stealer、AveMaria、LodaRAT、Meterpreter 等。感染鏈是由透過惡意垃圾郵件傳送的惡意附件。一旦開啟該附件，惡意 .LNK 檔將會呼叫 .HTA 網頁檔來下載惡意程式下載程式，然後下一階段再來下載有籌負載和惡意程式啟用程式到受感染的端點。

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.SuspDataRun
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen203
- Downloader
- Scr.Malcode!gdn32
- Scr.Mallnk!gen3
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2023/03/15

FiXS--全新ATM惡意軟體

FiXS 是一種全新 ATM 惡意軟體，觀察到在墨西哥的網路金融攻擊行動中被使用。根據最近的報導，FiXS 惡意軟體嵌入到 Neshta (Neshuta) 植入程式中。FiXS 攻擊 ATM 不限品牌，只要是支援 CEN／XFS（金融服務擴展）標準的 ATM 都有可能被入侵。惡意軟體可以等待 ATM 鈔箱裝入現金，然後再嘗試取款程序。它還具有允許在 ATM 重新啟動後嘗試分配現金之前延遲 30 分鐘的功能。攻擊者正在操控 FiXS 惡意軟體來透過外部鍵盤發送命令。

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
- W32.Neshuta
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS (data Center Security) 內建的應用程式控制政策可防止未經授權的程式執行並提供系統和應用程式鎖定以保護 ATM 免受 FiXS 惡意軟體等威脅。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/03/14

Prometei挖礦殭屍網路繼續在2023年壯大成長

Prometei 是過去幾年活躍於威脅領域的門羅幣 (XMR) 加密貨幣挖礦殭屍網路。營運商與時俱進更新殭屍網路功能並充分發揮基礎設施的綜效，目前最新 v3 版本的 Prometei 殭屍網路正在四處流通。值得一提的變化還包括自我更新機制、新的 C&C 動態網域產生演算法 (DGA，Domain Generation Algorithm)以及捆綁的 Apache Web 伺服器版本，其中包含可以傳送到受感染主機基於 PHP 的 Web shell。根據最近一份報告，這個殭屍網路的規模估計在全球約有 10,000 個受感染的系統。

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(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Mimikatz
- Infostealer!im
- Scr.Malcode!gdn32
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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 File SMB Request
- System Infected: Trojan.Backdoor Activity 335
- 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。

2023/03/13

防護亮點：Dark Power(*黑暗力量)勒索軟體

～防護亮點～

日以繼夜地持續監控勒索軟體駭客集團是賽門鐵克的核心任務，近期發現 Dark Power 駭客集團針對全球性跨國組織和企業提高其攻擊的力道與頻率。這個相對較新駭客集團透過在加密洋蔥網站上發布受害者名單來採用雙重勒索伎倆（這些是“暗網”網站，使用特殊軟體加密其連接並啟用匿名通訊以隱藏其位置和各種其他識別符）並威脅說，如果他們的贖金要求得不到滿足，他們就會出售被盜的資料。如果在受感染的電腦上加密成功，被加密檔將新增 .darkpower 副檔名。如果這個犯罪集團確實取得一定程度的成功，他們活動很可能會繼續並加劇。

Dark Power (*黑暗力量) 目前在以下國家／地區造成危害：

* 阿爾及利亞
* 捷克共和國
* 埃及
* 法國
* 以色列
* 秘魯
* 土而其
* 美國

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 **零時差**防護技術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.Ransomware!g1

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2023/03/13

Xenomorph最新版次v3行動惡意軟體，新增ATS框架的自動化功能

Xenomorph 是一種 Android 銀行惡意軟體，最初於 2022 年發現，歸因於網路犯罪集團--Hadoken Security Group。該惡意軟體的最新版本 v3 ，剛公諸於世，它增加一些新功能和優化。更重要的變化之一是新增 ATS 框架的自動化功能。ATS 代表自動轉帳系統，它允許駭客成員自動執行許多欺詐操作，而無需人員親自在現場或遠端操作或遠端。全新的 Xenomorph 版本還包含一個 cookie 竊取模組，用於從 Android CookieManager 中取得 cookie。

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。

- 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。

2023/03/13

ZK Java框架的CVE-2022-36537遠端程式碼執行(RCE)漏洞已經遭攻擊者開採利用

ZK Java 框架上的漏洞編號：CVE-2022-36537 是一個 2022 遠端程式碼執行 (RCE) 漏洞，已被評為高風險積分的 CVSS 等級。ZK 是一個基於 Java 的開放原始碼 Ajax 網頁應用程式開發框架，允許為網頁和手機 APP 建立圖形用戶界面。當該漏洞被開採利用，可能會導致資訊洩漏，但也可能允許潛在的攻擊者執行遠端程式碼。該漏洞在真實網路環境被開採利用後，美國網路安全暨基礎設施安全局（CISA）最近已將該漏洞收錄到「已知成功利用漏洞列表」。

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：

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: ZK Framework RCE CVE-2022-36537

2023/03/12

ScrubCrypt惡意軟體加密工具，開始被攻擊者拿來打包惡意挖礦程式

雖然加密貨幣的剪貼簿竊密器 (Clipper) 數量有所增加，但惡意挖礦程式仍然很普遍，並有報導稱惡意挖礦程式的攻擊行動有所增加。在最近一次攻擊行動中，他們開始在攻擊鏈中使用名為 ScrubCrypt 的惡意軟體加密工具，再交由 Bat 打包工具來打包。惡意軟體加密工具被世界各地的駭客組織與個體戶廣泛使用，並且可選擇的工具很多。這些惡意軟體主要的功能是透過加密惡意軟體中的惡意程式碼來逃避安全軟體的檢測。BAT 是常用的惡意程式打包加密技術。這種技術涉及將惡意程式碼壓縮成一個小的可執行檔，使用各種加密算法對其進行打包和加密。

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.maltraffic!gen1
- 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.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: Coinminer Activity 2
- System Infected: Miner.Bitcoinminer Activity 16
- System Infected: Trojan.Coinminer Activity 26

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。

2023/03/10

SYS01竊密程式鎖定臉書商業帳號

SYS01 惡意竊密程式，被利用於最近針對與政府機構和製造業等個別相關 Facebook 臉書商業帳號的攻擊行動中用。攻擊者利用 Google Ads 或虛假的 Facebook 個人資料將惡意酬載散發給毫無戒心的受害者。SYS01 Stealer 的主要功能是竊取機密資訊，例如：登錄憑證、Facebook 企業帳戶資訊、cookie 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：

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1
- SONAR.TCP!gen6

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

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／IP位址已於第一時間收錄於不安全分類列表中。

2023/03/10

會叫的狗未必會咬人～ALC恐嚇型的勒索軟體

ALC 是最近才出現在威脅領域的勒索軟體家族。該惡意軟體的行為更像是一個恐嚇軟體，因為它此時並沒有真正加密受感染系統上的任何檔案，而只是枚舉它們。這可能顯示該勒索軟體可能仍處於開發階段。ALC 會在受感染的系統上置放一個檔名為 AlcDif.exe 可執行檔，該檔案在執行時會把整個螢幕鎖定，並以全螢幕模式顯示勒索贖金支付說明，所以比較像是恐嚇軟體而非加密勒索軟體。

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：

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：

- Ransom.Gen
- 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.C

2023/03/10

賽門鐵克滴水不露的防護科技，完全完封CISA收錄「已知成功利用漏洞列表」

早在 2022 年揭露的三個漏洞已被美國網路安全暨基礎設施安全局（CISA）列為在真實網路環境已遭成功利用的高風險漏洞名單。

- **CVE-2022-28810** -- Zoho ManageEngine ADSelfService Plus 中的遠端程式碼執行漏洞(RCE)。此漏洞可能允許透過政策自定義腳本功能以 SYSTEM 身份執行任意操作系統命令。
- **CVE-2022-33891** -- Apache Spark 中的命令注入漏洞。利用此漏洞可能允許攻擊者在應用程序的上下文中執行任意程式碼。
- **CVE-2022-35914** -- Teclib GLPI 遠端程式碼執行漏洞 (RCE)。該漏洞存在於第三方函式庫 HTMLAWED 中，如果被利用可能允許 PHP 程式注入。

新增漏洞的 CVSS 評分範圍從中等到嚴重，已揭露的漏洞可能會給企業帶來重大風險。

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 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: Zoho ManageEngine ADSelfService Plus CVE-2022-28810
- Web Attack: Apache Spark CVE-2022-33891
- Web Attack: GLPI Unauthenticated RCE With Htmlawed Library CVE-2022-35914

2023/03/09

BianLian堪稱是最活躍的勒索軟體攻擊者之一

近幾個月來，BianLian 勒索軟體駭客集團磨刀霍霍，目標是跨國性的大型企業與組織。截至今天，該駭客集團是最活躍的犯罪組織之一，並採用雙重勒索伎倆，這意味著如果受害者不就範付贖金，就會將其資料公開或拍賣。

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
- Ransom.Bianlian!gm
- SONAR.PsDownloader!g1
- SONAR.SuspWrite!g6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Bianlian

基於機器學習的防禦技術：

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