保安資訊--本周(台灣時間2023/06/30)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 71 萬 2,500 台受保護端點上總共阻止了 8,820 萬次攻擊。這些攻擊中有 93% 在感染階段前就被有效阻止：**(2023/06/26)**

- 在**14萬800**台端點上，阻止了**3,620萬**次嘗試掃描**Web**服務器的漏洞。
- 在**23萬9,400**台端點上，阻止了**1,840萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**5萬1,800**台**Windows**伺服主機上，阻止了**1,410萬**次攻擊。
- 在**7萬8,100**台端點上，阻止了**240萬**次嘗試掃描伺服器漏洞。
- 在**1萬4,400**台端點上，阻止了**82萬5,400**次嘗試掃描在**CMS**漏洞。
- 在**5萬6,900**台端點上，阻止了**170萬**次嘗試利用的應用程式漏洞。
- 在**23萬2,600**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**1萬900**台端點上，阻止了**210萬**次加密貨幣挖礦攻擊。
- 在**14萬7,800**台端點上，阻止了**980萬**次向惡意軟體**C&C**連線的嘗試。
- 在**2,000**台端點上，阻止了**11萬900**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。

2023/06/29

CVE-2023-33246 Apache RocketMQ遠端程式碼執行(RCE)漏洞

CVE-2023-33246 是最近被披露的一個在 Apache RocketMQ 平台上嚴重等級（CVSS 評分：9.8）遠端程式碼執行 (RCE) 漏洞，該軟體是簡訊傳送和串流媒體平台 Apache RocketMQ 產品版本 5.1.0 及之前的版本中被發現該漏洞。如果該漏洞被利用開採，遠端攻擊者可以利用 RocketMQ 更新配置功能執行任意程式碼。Apache 已在產品版本 5.1.1 中發布緊急安全更新來解決此漏洞。

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：

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: RocketMQ RCE CVE-2023-33246

2023/06/29

NoName057(16)駭客組織利用DDosia工具組，繼續進行DDoS攻擊

DDosia 是一種殭屍網路惡意軟體，在過去幾個月中，NoName057(16) 駭客組織利用該惡意軟體對歐洲各國政府機構、團體和私營公司的網站發起一系列分散式拒絕服務 (DDoS) 攻擊。眾所周知，NoName057(16) 歹徒將攻擊重點放在烏克蘭或支持烏克蘭的國家和組織。DDosia 惡意軟體有多種版本，可支持包括 Windows、Linux 和 macOS 等不同的作業系統。DDosia 惡意軟體也透過歹徒操控的 Telegram 頻道進行傳播。僅上個月就顯示攻擊者頻道的訂閱者數量大幅增加，並且利用 DDosia 工具組發動 DDoS 攻擊的駭客數量也有所增加。

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
- OSX.Trojan.Gen
- 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。

2023/06/29

影響VMware Aria Operations for Networks的CVE-2023-20887漏洞

CVE-2023-20887 是最近被披露的一個嚴重等級（CVSS 評分：9.8）命令注入漏洞，影響 VMware Aria Operations for Networks（一種網路監控和管理解決方案）。如果該漏洞被開採利用，未經身份驗證的攻擊者可以在不需要用戶互動下，執行任意程式碼。可開採利用該漏洞的程式碼已被公開發布，並且該漏洞也被報告為已被開採利用。VMWare 已發布緊急安全產品更新來解決此漏洞。

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：

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: VMware Aria Operations for Networks CVE-2023-20887

2023/06/29

Linux平台也出現Akira勒索軟體

Akira 勒索軟體，於 2023 年 4 月首次出現在真實網路環境中。雖然最初僅觀察到該勒索軟體只有 Windows 版本，但現在也出現 Linux 版本。該勒索軟體會針對預先定義的特定附檔名的檔案進行加密--許多檔案與虛擬化 VMware ESXi 環境相關。成功加密後，被加密的檔案會被冠上 .akira 的副檔名，並將勒索贖金支付說明訊息存放到受感染的系統上。

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

基於安全強化政策(適用於使用DCS)：

Symantec Data Center Security (DCS) 預設的強化政策可提供針對 Akira 勒索軟體的零時差保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/06/29

又是雙重勒索手法～8Base勒索軟體

據報導，自 2023 年 5 月以來，與 8Base 勒索軟體組織相關的惡意活動有所增加。8Base 勒索軟體可能是眾所周知的 Phobos 勒索軟體的分支，因為這兩種惡意軟體之間有許多相似之處。8Base 背後的組織也可能與鮮為人知的 RansomHouse 駭客組織有關--同樣這裡也有一些相似之處，例如：兩個駭客組織所存置的贖金支付說明。被 8Base 勒索軟體加密的檔案會被冠上 .8base 副檔名。歹徒集團還建立一個公開洩密網站，大肆宣傳遭受此勒索軟體危害的受害者公司。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

2023/06/26

防護亮點：LockBit--多產、持久、可預防

~ 防護亮點 ~

LockBit 是一種勒索軟體即服務 (RaaS)，早在 2019 年 9 月就由賽門鐵克追踪為 Syrphid 的駭客集團所營運。它攻擊不同規模的組織，包括但不限於金融服務、專業服務、食品和農業、法律、教育、能源、緊急服務、醫療保健、製造和運輸，據信迄今為止共發動多達 1,700 起的網路攻擊，其中 1 起在 2022 年期間發生 6 組駭客一起針對美國政府的勒索軟體攻擊。LockBit 採用勒索軟體即服務 (RaaS) 營運模式，招募新的聯盟夥伴使用 LockBit 勒索軟體工具和基礎設施進行攻擊。這種多樣化的聯盟夥伴導致 LockBit 勒索軟體攻擊在其觀察到的戰術、技巧，以及程序 (TTPs) 等面向差異很大，使得組織更難以防禦。

LockBit 多年來不斷發展。最初在 2019 年首次發佈時稱自己為「ABCD 勒索軟體」，該聯盟夥伴計劃於 2020 年 1 月推出，然後 2020 年 9 月推出一個洩漏網站（其中列出拒絕支付贖金的受

感染組織），LockBit 也採用雙重勒索戰術。2021 年，LockBit 2.0 開採利用一個名為 CVE-2018-13379 的陳年漏洞，針對澳洲亞組織。到 2021 年底，發布一個針對 VMware ESXi 虛擬機的 Linux 變種。2022 年 6 月出現 3.0 變種由於程式碼與 BlackMatter 和 Darkside 勒索軟體變種相似，因此被稱為「LockBit Black」。LockBit 3.0 可以刪除許多預定義的服務並終止某些程序。

同年 7 月，攻擊者被發現使用名為 Terminator 的工具來嘗試停用安全軟體。這些類型的攻擊就是利用含有弱點的驅動程式檔案，進行自帶驅動程式攻擊（BYOVD：Bring Your Own Vulnerable Driver），涉及使用有效數位簽章的合法驅動程式，這些驅動程式能夠執行特權指令，並被植入到受害者設備上以停用安全解決方案並接管系統。

賽門鐵克用戶應注意，只有當攻擊者擁有管理憑證並且 SEP 管理員已停用防篡改保護時，任何嘗試停止 SEP 的命令或工具才會起作用。

就在今年 4 月，還發現一種針對 macOS 平台的新 LockBit 變種，這些樣本似乎基於 LockBit 的 Linux 加密器，並且僅針對 macOS 進行編譯。來自安全研究人員的最新情報是，LockBit 操作似乎已經開始試驗其有效籌載的新版本，能夠攻擊多種架構，包括 Apple M1、ARM v6、ARM v7、FreeBSD 等。

像 LockBit 這樣危險且不斷演變的威脅需要同樣積極的回應。

賽門鐵克針對 LockBit 的眾多變種及其各個組件提供了**全面的保護**：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- OSX.Ransom.Lockbit
- Packed.Generic.686
- Ransom.Lockbit
- Ransom.Lockbit!g1
- Ransom.Lockbit!g2
- Ransom.Lockbit!g6
- Ransom.Lockbit!g7
- Ransom.Lockbit!gen3
- Ransom.Lockbit!gen4
- Ransom.Lockbit!gen5
- Ransom.Lockbit!gm1
- Scr.Malscript!gen1
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1

基於行為偵測技術(SONAR)的防護：

- Ransom.Blackmater!gm1
- SONAR.Cryptlocker!g42
- SONAR.ProcHijack!gen5
- SONAR.ProcHijack!g45
- SONAR.Ransomware!g2
- SONAR.Ransomware!g7
- SONAR.RansomLckbit!g1
- SONAR.RansomLckbit!g2
- SONAR.RansomLckbit!g3
- SONAR.RansomLckbit!g4
- SONAR.RansomLckbit!g5
- SONAR.RansomNokibi!g1
- SONAR.SuspBeh!gen82
- SONAR.SuspBeh!gen742
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!gen18
- SONAR.SuspLaunch!g189
- SONAR.SuspLaunch!g190
- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g195
- SONAR.SuspLaunch!g253
- SONAR.SuspReg!gen28
- SONAR.UACBypass!gen30

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.C
- 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：

- Attack: Ransom.Lockbit Activity
- Attack: Ransom.Lockbit Activity 2
- Attack: Ransom.Lockbit Activity 3
- Web Attack: Webpulse Bad Reputation Domain Request
- Web Attack: Fortinet FortiOS Directory Traversal CVE-2018-13379
- Attack: Lockbit Ransomware Binary Copy GPO Config

- Attack: Lockbit Ransomware Enable Share GPO Config
- Attack: Lockbit Ransomware Security Services Taskkill GPO
- Attack: Lockbit Ransomware Services Disable GPO Config

基於安全強化政策(適用於使用DCS)：

- DCS 內建的強化政策可針對 LockBit 勒索軟體的零時差保護。
- 可疑程序執行：預防策略防止惡意軟體在系統上被植入或執行。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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)。

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。

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。
欲瞭解更多有關於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。
欲瞭解有關於賽門鐵克(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。
欲瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請單擊此處。

2023/06/26

FluHorse手機行動裝置惡意軟體，不斷提升技術

網路釣魚氾濫早已不足為奇，藉由使用各種可客製化的網路釣魚工具套件，網路犯罪分子不斷改變其戰術、技巧，以及程序（TTPs），以期逃避惡意垃圾郵件檢測。Fluhorse 是源於被稱為 Flutter 的開放原始碼框架所開發，於 2023 年 5 月首次被報導。然而，今年 6 月，藉由假冒知名的 APP，該網路釣魚行動背後的歹徒已將其技術從基本混淆轉向打包和隱藏可執行檔中的加密有效籌載。歹徒模仿東亞合法金融機構或收費公司的熱門 APP，下載量已達數百萬次。FluHorse 惡意軟體的目標是竊取憑證、雙因素身份驗證 (2FA) 碼和信用卡資訊等。

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：

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：

- Android.Malapp
- Android.Reputation.2
- Trojan.Gen.MBT

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

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。

2023/06/26

《超級馬里奧 3：永遠的馬里奧》電玩安裝程式，被暗中植入木馬

被暗中植入木馬的《超級馬里奧 3：永遠的馬里奧》安裝程序被發現會帶來多種威脅，包括門羅幣 (XMR) 挖礦程式、SupremeBot 挖礦用戶端和源於開放原始碼的Umbral 竊密程式。惡意軟體安裝套件與合法安裝程式捆綁在一起，以隱藏其存在。濫用受害者的電腦來挖礦是歹徒的主要目標。

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

基於機器學習的防禦技術：

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