保安資訊--今日最新(台灣時間2024/10/15)
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 45 萬 100 台受保護端點上總共阻止了 4,770 萬次攻擊。這些攻擊中有 81.1% 在感染階段前就被有效阻止：**(2024/10/14)**

- 在**9**萬**2,900**台端點上，阻止了**1,420**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11**萬**600**台端點上，阻止了**870**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3**萬台**Windows**伺服主機上，阻止了**7**萬**1,000**次攻擊。
- 在**6**萬**200**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**600**台端點上，阻止了**72**萬**9,300**次嘗試掃描在**CMS**漏洞。
- 在**5**萬**300**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**14**萬**1,500**台端點上，阻止了**290**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,000**台端點上，阻止了**100**萬次加密貨幣挖礦攻擊。
- 在**10**萬**4,600**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**529**台端點上，阻止了**9**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。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點 (桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在 18 萬 7,000 個受保護端點上阻止了總計 750 萬次攻擊。**(2024/10/14)**

- 使用網頁信譽情資，在 **177.6K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **22.2K** 個端點上 **278K** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在 **8.8K** 個端點上攔截 **116.8K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在 **454** 個端點上攔截 **9.7K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

點擊此處獲取--關於賽門鐵克原廠防護週報

2024/10/14

Demodex惡意軟體持續涉入針對美國電信供應商的網路攻擊

根據報導，進階持續威脅 (APT) 駭客組織--「Squash」正在利用 Demodex 惡意軟體，針對美國電信供應商，發動網路攻擊。Demodex 是一種用來建立持久性／常駐能力的 rootkit，再用帶有虛假檔案標頭 (已發現到 PNG、JPEG 和 WAV) 的檔案來協助躲避偵測，並用來建立 C&C 通訊。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.A!400
- Heur.AdvML.A!500
- Heur.AdvML.C

2024/10/14

CVE-2024-43573--存在微軟視窗環境的MSHTML平臺欺騙漏洞

CVE-2024-43573 是存在微軟視窗環境的 MSHTML 平臺欺騙漏洞，最近被披露並已在微軟發布的 10 月例行更新 (Patch Tuesday) 中推出修補程式。此漏洞會影響 Microsoft Windows MSHTML 平台。此漏洞的 CVSS 風險評分 6.5 (中度)，攻擊者可在運行受影響應用程式的情境中執行任意程式碼。CVE-2024-43573 漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，之前也曾有報告指出有人在真實網路情境上大肆開採濫用此漏洞。

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: Windows MSHTML Platform CVE-2024-43573

基於安全強化政策(適用於使用DCS)：

針對此漏洞提供如下的多層級保護：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security，可以對 Microsoft Internet Explorer 的預設強化提供針對 CVE-2024-43573 的零時差防護。在預設強化政策中，所有向外連線都會被封鎖。
- 套用於 Microsoft IE 的 DCS 沙箱可防止下載任何惡意有效酬載或執行任意程序。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/10/14

全新Pronsis惡意程式載入器，涉入傳遞Lumma惡意竊密程式和Latrodectus有效酬載荷的網路攻擊行動中嶄露頭角

全新 Pronsis 惡意程式載入器，最近在涉入傳遞 Lumma 惡意竊密程式和 Latrodectus 有效酬載荷的網路攻擊行動中嶄露頭角。Pronsis 是採用 JPHP 程式語言編譯的可執行檔，這是 PHP 的 Java 實作。已發現的攻擊事件中發現，Pronsis 也使用 Nullsoft Scriptable Install System (NSIS) 來部署。該惡意軟體具有多種偵測規避技術，例如：從 Windows Defender 掃描中排除使用者設定檔目錄路徑。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-FlPst!g1
- ACM.Ps-Java!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.SuspRename!g4
- SONAR.TCP!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- MSIL.Downloader!gen8
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Startpage
- W32.Silly!gen
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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：

- Audit: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 634
- 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。

2024/10/11

LemonDuck：越來越大尾的多平臺挖礦惡意軟體

LemonDuck 是一款知名的挖掘惡意軟體，已演變成多平台威脅，且被發現到利用 SMB 漏洞作為其攻擊媒介的一部分，尤其是 EternalBlue，以取得網路存取權限。該惡意軟體採用的技術包括暴力攻擊、建立隱藏的管理共用，以及透過批次檔案和 PowerShell 腳本執行惡意動作。LemonDuck 具備建立排程任務、停用 Windows Defender，以及利用反偵測機制持續作業的能力。它會偽裝成合法的系統服務，操控防火牆設定，此外還會使用密碼提取工具：Mimikatz 來盜取憑證。

網路上的知識：EternalBlue 是一個 Windows Server Message Block(SMB) 協議中的漏洞，該漏洞允許攻擊者在無需用戶交互的情況下，遠端執行任意代碼。開採濫用 EternalBlue 漏洞，攻擊者可以輕鬆地在未修補的 Windows 系統上植入惡意程式碼，並進一步擴散到網路中其他設備。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Wscr-Cmd!g1
- ACM.Wscr-Ps!g1
- ACM.Wscr-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g393

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Remacc.Remadmin
- CL.Downloader!gen9
- WS.Malware.2

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：

- Audit: Impacket Tool Activity
- Audit: RADMIN Tool Activity
- Audit: Powershell Base64 Script Execution 02

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。

2024/10/11

CVE-2024-7954--存在SPIP Porte Plume外掛程式的遠端執行程式碼漏洞

CVE-2024-7954 是存在 SPIP 4.30-alpha2、4.2.13 及 4.1.16 之前版本所使用 porte_plume 外掛程式中的遠端執行程式碼 (RCE) 嚴重等級 (CVSS 風險評分：9.8) 的漏洞。SPIP 是用於發布內容管理系統 (CMS) 網站的免費軟體。此漏洞可能會允許未認證的遠端攻擊者傳送特製 HTTP 請求，並以 SPIP 使用者身份執行任意 PHP 程式碼。此攻擊可完全入侵伺服器以竊取機密資訊，並轉向內部網路。賽門鐵克端點防護的多層防護技術之一網路層防護技術的入侵防護系統 (IPS) 可阻止這些漏洞利用嘗試，以防止系統受到進一步感染／損害。

網路上的知識：SPIP 是一種用於網際網路的發佈系統，非常重視協作工作、多語言環境以及網頁作者的簡易使用。它是自由軟體，根據 GNU／GPL 許可證分發。

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: SPIP Porte Plume Plugin RCE Vulnerability CVE-2024-7954

2024/10/11

Lynx勒索軟體--讓人毛骨悚然的網路勒索威脅

Palo Alto Networks Unit 42 發表最新研究指出，被稱為 Lynx 勒索軟體最新變種與 INC 勒索軟體共用大部分的原始碼。Lynx 營運商已積極鎖定美國和英國的各行各業 (建築、房地產、零售和金融／環境服務) 的組織為目標。此勒索軟體採勒索軟體即服務 (RaaS) 的營運模式，並透過各種攻擊媒介 (欺騙性的釣魚郵件、感染使用者系統的惡意下載以及駭客論壇等) 散播。一旦感染 Lynx 勒索軟體，受害者的資料會在加密前先被滲出，然後採用雙重勒索的戰術來脅迫受害者以提高就範率。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomPlay!gen1
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7
- SONAR.Ransomware!g38
- SONAR.Ransom!gen14
- SONAR.Ransom!gen98

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Ransom.Gen
- Ransom.Inc
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.2
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。

2024/10/11

CVE-2024-43572--存在微軟Windows管理主控臺(MMC)的遠端執行程式碼(RCE)類型的漏洞

CVE-2024-43572 是存在微軟 Windows 管理主控臺 (MMC) 遠端執行程式碼 (RCE) 類型的漏洞，最近被披露並已在微軟發布的 10 月例行更新 (Patch Tuesday) 中推出修補程式。此漏洞可透過執行特製的惡意 Microsoft Saved Console (MSC) 檔案利用。成功開採濫用此漏洞可讓攻擊者在執行應用程式的情境執行任意程式碼。CVE-2024-43572 漏洞也已被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，之前也曾有報告指出有人在真實網路情境上大肆開採濫用此漏洞。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLoad!g65

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Suspexec!gen50
- Trojan Horse

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。

2024/10/11

Apache RocketMQ的已知漏洞CVE-2023-33246，已被Perfctl惡意軟體開採濫用以攻擊全球Linux伺服器

已發現到針對全球數百萬台 Linux 伺服器的 Perfctl 惡意軟體攻擊行動。該行動開採濫用分散式訊息串流資料平臺 Apache RocketMQ 的已知漏洞 CVE-2023-33246。該惡意軟體利用 rootkits 進行隱身和程序偽裝，並利用洋蔥路由器加密通訊 (TOR) 與命令和控制 (C&C) 伺服器通訊。最終有效酬載，是部署挖礦程式和代理劫持軟體。此外，惡意軟體利用暫存目錄和修改過的系統公用程式來逃避偵測。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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
- PUA.Gen.2
- WS.Malware.2

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

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。

2024/10/11

偽裝成《Honkai：Star Rail／*崩壞：星穹鐵道》的安裝程式～Kransom勒索軟體以遊戲玩家為目標

有報告指出，一款名為 Kransom 的全新勒索軟體正在利用《Honkai: Star Rail／*崩壞：星穹鐵道》這款受歡迎的多平台銀河冒險角色扮演遊戲。該勒索軟體透過隨機下載行動進行傳播，將惡意的二進位檔偽裝成合法的 Star Rail 遊戲安裝程式，且使用有效的數位憑證，進而誘騙受害者。執行時，惡意 DLL 會使用動態連結庫 (DLL) 側載技術載入，啟動勒索軟體的加密程序。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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。