保安資訊--本周(台灣時間2024/07/05)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 50 萬 2,100 台受保護端點上總共阻止了 5,010 萬次攻擊。這些攻擊中有 81.4% 在感染階段前就被有效阻止：**(2024/07/01)**

- 在**10萬7,000**台端點上，阻止了**1,380**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**12萬5,900**台端點上，阻止了**990**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,000**台**Windows**伺服主機上，阻止了**890**萬次攻擊。
- 在**5萬7,300**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,400**台端點上，阻止了**76萬4,900**次嘗試掃描在**CMS**漏洞。
- 在**5萬5,900**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**16萬5,400**台端點上，阻止了**410**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,700**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬1,900**台端點上，阻止了**820**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**605**台端點上，阻止了**10萬5,000**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 11 萬 9,200 個受保護端點上阻止了總計570 萬次攻擊。**(2024/07/01)**

- 使用網頁信譽情資，在 **109.4K** 個端點上阻止 **520** 萬次攻擊。
- 攔截 **22.3K** 個端點上 **368.3K** 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 **7.3K** 個端點上攔截 **76.6K** 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 **234** 個端點上攔截 **10.2K** 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。

2024/07/05
Mekotio惡意軟體針對拉丁美洲的銀行客戶

Mekotio 是一種銀行金融木馬，至少從 2015 年起就活躍在威脅領域，主要針對拉丁美洲地區。根據趨勢科技發佈的最新報告，最近在真實網路情境上觀察到傳播這種惡意軟體的攻擊激增。Mekotio 的功能包括系統資訊收集、銀行憑證外洩、鍵盤側錄、剪貼簿資料竊取和螢幕截圖等。該惡意軟體能夠顯示模仿合法銀行入口網站的假快顯視窗，進而誘騙受害者輸入並洩露其銀行帳號等詳細資訊。

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：

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.Gen.MBT
- Trojan.Gen.NPE

- WS.Malware.1
- Web.Reputation.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

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。

2024/07/04
以宗教為誘餌：AndroRAT以奈及利亞行動用戶為目標

奈及利亞是一個宗教氛圍濃厚的國家，有多種不同的信仰。但宗教在奈及利亞的重大影響，也為針對消費者和企業的社交工程攻擊提供滋生矇混騙術的溫床。在最近一個案例中，賽門鐵克發現有人試圖用一個偽造的古蘭經相關 APP(AssunnahQuranApp.apk) 引誘奈及利亞行動用戶，而這個 APP 實際上是偽裝的 AndroRAT。

AndroRAT 是一種安卓平台上的遠端存取工具 (RAT)，透過用戶端--伺服器的模式運行，允許遠端攻擊者在安裝後控制受害者的手機。包括存取位置、通話記錄和連絡人等資料，以及執行發送簡訊或拍照等操作。

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.1

2024/07/04
偽造土耳其名人的性愛錄影帶助長SpyNote傳播

偽造性愛錄影帶仍是惡意軟體傳播常用的社交工程誘餌，因為它們能夠喚起強烈的情感，有可能導致衝動行為。這類內容吸引廣大受眾，利用人類好奇心和對社會汙名的恐懼，使人們更有可能接觸這些素材，以求證其真實性或試圖將其刪除。

最近，賽門鐵克發現針對土耳其行動用戶的偽造性愛錄影帶數量有所增加。一個團體或個人正在將一個著名的遠端存取木馬 (SpyNote) 偽裝成看似 MP4 影片檔的 Android APP(例如：[名人姓名][露骨語言].mp4.apk)。在社交工程攻擊中，他們使用土耳其著名女演員、歌手和其他名人的名字，誘騙使用者下載 APP 並在其手機上執行。

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
- Android.Reputation.1

2024/07/04
軟體開發業者JetBrains存在整合開發環境(IDE)IntelliJ平臺的漏洞：CVE-2024-37051

CVE-2024-37051 是最近披露一個影響 Jetbrains IntelliJ 整合式開發環境 (IDE) 應用程式的關鍵漏洞。如果開採濫用該漏洞，攻擊者可能會暴露 GitHub 存取權杖，並在未經授權的情況下存取 Github 資源。JetBrains 已經發佈安全更新來解決這個漏洞。

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: JetBrains IDEs GitHub Plugin CVE-2024-37051

2024/07/04
Volcano Demon駭客組織所傳播的LukaLocker勒索軟體

LukaLocker 是一個名為 Volcano Demon 勒索軟體組織新近推出的產品。最近觀察到的攻擊，初始階段是使用擷取的憑證來進行後續資料滲出。在攻擊中發現以下行徑：

- 透過資料外滲和檔案加密進行雙重勒索
- 加密檔的副檔名為 .nba
- 不同應用程式類型 (安全軟體、資料庫、虛擬化等) 的程序和服務會被終止。

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.Ransomware!g7

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- Trojan Horse
- Trojan.KillAV

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/07/03

偽裝成電子書來散播的AsyncRAT惡意軟體

早先報告詳細介紹 AsyncRAT 惡意軟體通常是如何透過 .chm、.wsf 和 .lnk 等檔副檔名傳播。攻擊者將惡意軟體偽裝成文件檔中『調查』內容，最近又偽裝成電子書。欺騙性的電子書檔案包含一個惡意 LNK 檔，並偽裝成一個壓縮圖示，會觸發一個 PowerShell 腳本 (RM.TXT)，還有一個偽裝影片檔和合法的電子書。這些伎倆凸顯利用看似無害的檔案騙取用戶信任的老練方法。

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：

- Scr.Malcode!gdn14
- Scr.Malcode!gdn32
- 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.A!300
- Heur.AdvML.B
- 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。

2024/07/03

CosmicSting(CVE-2024-34102)--XXE漏洞針對Adobe Commerce和Magento

CVE-2024-34102 是 Adobe commerce 和 Magento(熱門的電商平臺) 中一個嚴重等級 (CVSS風險評分：9.8) XML External Entity Reference (XXE) 漏洞。此問題源於巢狀反序列化處理不當，導致任意程式碼執行。攻擊者可透過發送引用外部實體的偽造 XML 檔來開採利用此漏洞。如果成功開採利用此漏洞，未經認證的攻擊者就可以存取敏感檔案，進而可能導致資料被盜、服務中斷以及受影響系統的完全崩潰。賽門鐵克端點防護的網路層防護技術入侵防護系統 (IPS) 可阻止這些漏洞利用嘗試，以防止對系統造成進一步感染／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：

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: Adobe Commerce XXE Vulnerability CVE-2024-34102

基於安全強化政策(適用於使用DCS)：

針對 Adobe Commerce 和 Magento 應用程式的 DCS 強化可透過多種不同方式減少攻擊面和暴露：

- 鎖定易受攻擊的應用程式的網路暴露，這樣就無法透過網際網路開採利用相關漏洞，例如：magneto 的此遠端 CVE 或類似遠端 CVE。
- 防止存取底層作業系統檔上的作業系統關鍵檔案，進而防止敏感系統資訊洩漏 (本 POC 中的 /etc/passwd)。
- 防止任意程式碼執行，防止惡意子程序譜系。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/03

CVE-2024-29849--Veeam Backup Enterprise Manager身份驗證繞過漏洞

CVE-2024-29849 是最近披露一個影響 Veeam Backup Enterprise Manager 的關鍵身份驗證旁路漏洞 (CVSS 風險評分：9.8)。成功開採濫用該漏洞可使攻擊者繞過身份驗證，進而在受影響應用程式的使用情境中執行任意程式碼。除了供應商提供的幾個緩解步驟外，該漏洞已在發佈的軟體更新版本 12.1.2.172 中得到解決。

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: Veeam Backup Enterprise Manager CVE-2024-29849

2024/07/03
CVE-2024-36104--Apache OFBiz中的路徑遍歷漏洞

CVE-2024-36104 是存在 Apache OFBiz 中路徑遍歷漏洞。由於對 HTTP 請求網址中的特殊字元(例如：;、%2e) 限制不當，威脅者可建立惡意請求來開採濫用此漏洞。如果被開採濫用，遠端攻擊者可在未經授權的情況下存取機敏檔案或目錄，並可能導致遠端程式碼執行。此問題會影響 Apache OFBiz 18.12.14 之前的版本。賽門鐵克端點防護的網路層防護技術入侵防護系統 (IPS) 會阻擋這些漏洞的攻擊嘗試，以防止系統受到進一步感染或損害。

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: Apache OFBiz Path Traversal Vulnerability CVE-2024-36104
- Web Attack: Apache OFBiz Path Traversal Vulnerability CVE-2024-36104 2

基於安全強化政策(適用於使用DCS)：

針對 Apache OFBiz 應用程式的 DCS 強化可透過多種不同方式減少攻擊面和暴露：

- 鎖定 OFBiz 網路暴露，這樣就無法透過網際網路利用 Apache OFBiz 這個或類似遠端漏洞。
- 防止存取底層作業系統上的作業系統關鍵檔案，進而防止敏感的系統資訊洩漏。
- 防止任意程式碼執行，以防止惡意子程序譜系。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/03
k4spreader：中國駭客組織「8220」使用的新型惡意軟體工具

據觀察，「8220」中國威脅組織在最近行動中使用一種名為 k4spreader 的新型惡意軟體工具。k4spreader 用 cgo 撰寫，具有系統常駐能力、自我下載和更新能力等功能，還能部署從命令與控制 (C&C) 伺服器下載 Tsunami DDoS 殭屍網路和 PwnRig 挖礦程式等其他惡意軟體。K4spreader 似乎仍在不斷改進，迄今已觀察到三個版本。。

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：

- Linux.Backdoor.Kaiten
- Linux.Trojan
- PUA.Gen.2

- 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。

2024/07/02

OpenSSH中存在『regreSSHion』漏洞 (CVE-2024-6387)

賽門鐵克發現 OpenSSH 中存在『regreSSHion』漏洞 (CVE-2024-6387)，這是一個嚴重等級的遠端程式碼執行 (RCE) 漏洞。根據最近的報告，這其實是個回歸漏洞，這意味著它在之前被修補後再次出現，並與 CVE-2006-5051 有關。

此漏洞影響 OpenSSH 4.4p1 及 8.5p1 至 9.8p1 版本。它利用 SSH 伺服器 (sshd) 中的訊號處理器競爭條件，允許未經授權的遠端攻擊者執行任意程式碼。該問題主要影響在基於 glibc 系統上執行的 Linux 發行版本，緩解措施包括更新到最新版本的 OpenSSH(9.8p1 或更高版本)。

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：

基於安全強化政策(適用於使用DCS)：

賽門鐵克重要主機防護系統：DCS～Data Center Security，針對此漏洞提供如下多層級保護：

- 針對 Linux 伺服器的賽門鐵克 DCS 預設預防政策 sym_unix_protection_sbp，可在安全沙箱 (Default Daemon Sandbox，int_gateway_ps) 中強化 OpenSSH 伺服器保護程序 (sshd)，保護關鍵作業系統資源。此外，DCS Linux prevention policy 預設鎖定 root 用戶帳戶，防止潛在威脅利用此漏洞濫用管理權限，以 root 身份在伺服器上執行遠端程式碼。客戶可利用 Default Daemon Sandbox 中的網路強化規則確保 sshd 保護程序的安全，使其僅接受來自受信任來源的用戶端連線。
- DCS 預設的 UNIX Baseline Detection policy 會對多次以 root 用戶身份登錄 ssh 的失敗嘗試發出警報，進而為未經授權入侵 Linux 伺服器提供早期預警能見度。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/02

防護亮點：SEP第一時間有效攔截漏洞開採利用～程式語言 PHP 存在PHP-CGI引數注入(Argument Injection)漏洞：CVE-2024-4577

程式語言 PHP 存在 PHP-CGI 引數注入 (Argument Injection) 漏洞：CVE-2024-4577， 正在被大肆開採濫用

PHP 是一種通用伺服器指令碼語言，是製作動態互動式網頁的強大腳本工具。CVE-2024-4577 是一個高嚴重性等級 (CVSS風險評分：9.8) 的參數注入漏洞，當 PHP 以 CGI 模式執行時會受到影響。該漏洞是由於在 Windows 上執行 PHP 時失誤造成的，特別是與程式碼轉換 Best-Fit 功能相關。如成功開採濫用此漏洞，未經認證的攻擊者可在受影響的 PHP 伺服器上執行任意程式碼，導致系統被完全入侵及隨後的惡意軟體傳遞。由於 PHP 是一種廣泛使用的指令碼語言，攻擊者很快就開始利用這一漏洞入侵網路並部署不同類型的惡意軟體有效酬載。有證據顯示該漏洞被大肆開採濫用後，美國網路安全暨基礎設施安全局 (CISA) 最近將該漏洞新增到「已知成功

利用漏洞列表 (the Known Exploited Vulnerabilities Catalog-KEV)」目錄中。

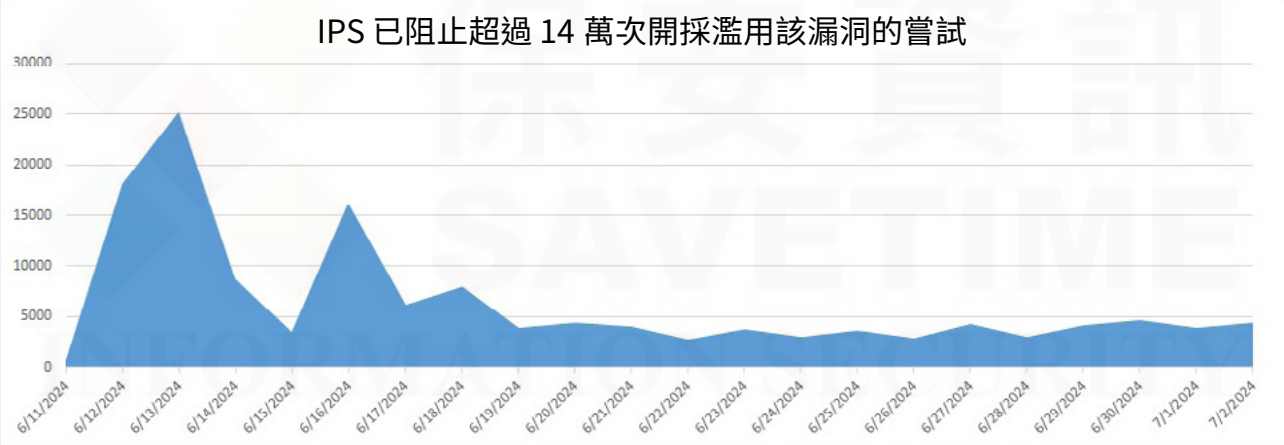
觀察到的惡意軟體有效酬載

賽門鐵克已觀察到威脅行為者利用此漏洞後發送的以下惡意軟體有效酬載：

- TellYouThePass 勒索軟體，它會加密系統中的檔案，使其無法使用
- Web shell 有效酬載，用於獲取受攻擊電腦的後門存取權限
- 流行的威脅模擬工具 CobaltStrike
- 在被入侵的 Windows 機器上進行挖礦劫持
- Mirai 殭屍網路，主要在劫持物聯網 (IoT) 設備並將其接管變成遠端控制的『機器人』

賽門鐵克的防護技術集

賽門鐵克端點防護上的網路層防護技術：入侵防護系統 (IPS) 與賽門鐵克其他多層次防護技術的協同防護架構，可阻止這些漏洞利用嘗試，防止系統受到感染／破壞。IPS 在初始階段就能阻止攻擊，進而確保不會向系統注入惡意有效酬載。迄今為止，IPS 已阻止超過 14 萬次開採濫用該漏洞的嘗試。



研究人員發現 PHP 存在引數注入 (Argument Injection) 漏洞 (CVE-2024-4577)，未經身分鑑別之遠端攻擊者，可透過特定字元序列繞過舊有 CVE-2012-1823 弱點修補後之保護，並透過引數注入等攻擊於遠端 PHP 伺服器上執行任意程式碼，請儘速確認並進行修補。

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
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspScript!g7
- SONAR.SuspLaunch!g18

- SONAR.Downloader!gen2
- SONAR.Trafic1.RGC!g10
- SONAR.Dropper

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：

- Ransom.Gen
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.MBT
- Hacktool.Mimikatz
- WS.Malware.1
- Backdoor.Doublepulsar
- IRC.Backdoor.Trojan
- Backdoor.Cobalt
- Linux.Trojan

基於機器學習的防禦技術：

- 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：

- Web Attack: PHP-CGI Argument Injection Vulnerability CVE-2024-4577
- Web Attack: Malicious Payload Download 21

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。
賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。
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，請點擊此處。

2024/07/02

以Apple ID為目標的簡訊網路釣魚行動，正在美國大肆散播

由於 Apple ID 被廣泛使用，可以接觸到大量的潛在受害者，因此網路釣客持續將 Apple ID 作為攻擊目標。這些憑證價值很高，可以控制裝置、存取個人和財務資訊，並透過未經授權的線上交易獲得潛在收入。此外，Apple 強大的品牌商譽讓用戶更容易相信看似來自 Apple 的詐騙性通訊，進一步增強這些潛在受害者成為網路釣客覬覦的吸引力。

這些行動大多透過電子郵件進行，但也越來越多透過惡意簡訊進行。在最近一個案例中，一個威脅行為者在美國發佈惡意簡訊。

觀察到的惡意簡訊：

- Apple 重要請求 iCloud：登入 signin[.]authen-connexion[.]info/icloud 以繼續使用您的服務。(Apple important request iCloud: Visit signin[.]authen-connexion[.]info/icloud to continue using your services.)

通常，簡訊網路釣客會限制手機上瀏覽器和特定地區的使用者瀏覽其惡意網站，以逃避監控系統的檢測。然而，在這種情況下，惡意網站既可以透過桌上型電腦瀏覽器瀏覽，也可以透過手機瀏覽器瀏覽。為了增加可信度，他們也會使用驗證碼，用戶必須完成驗證。之後，用戶會被導引到一個模仿舊版 iCloud 登錄範本的網頁。

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。WebPulse 已知此活動中使用的假 Apple 網域。

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。

2024/07/02

CVE-2024-31982--XWiki平台存在端程式碼執行(RCE)漏洞

CVE-2024-31982 是一個最近披露的遠端程式碼執行 (RCE) 漏洞，影響 XWiki，它是一個主流基於 Java 的開源 wiki 平臺。該漏洞可能允許攻擊者透過資料庫搜索功能遠端執行任意程式碼。入侵者可能會導致資料洩露並接管存在漏洞的 XWiki 實例。該漏洞已在已發佈更新產品版本 14.10.20、15.5.4 和 15.10-rc-1 中得到修補。

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: XWiki RCE CVE-2024-31982

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，其出廠就內建的系統鎖定政策，可以防止在相關程序的伺服器上被部署可疑的 web shell，更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。
- DCS 預設的鎖定政策可保護底層 UNIX 伺服器免受此漏洞的影響，包括防止執行任意命令和限制讀取主要的作業系統檔案。

2024/07/01

Datebug進階持續威脅(APT)駭客組織持續傳播CapraRAT安卓惡意軟體

根據 Sentinel One 研究人員的報告，與 Datebug 進階持續威脅 (APT)(又名 Transparent Tribe 或 APT36) 駭客組織相關惡意活動有捲土重來的態勢。這些威脅行為者持續模仿像極合法 APP 的惡意 .apk 安卓平台上安裝包來散播 CapraRAT 惡意軟體。據了解，Datebug 駭客組織一直以印度軍事和政府部門的個人為目標，而最近行動則利用一些新的誘餌，並試圖將觸角伸向對手機遊戲感興趣、喜歡 TikTok 影片或武器狂熱分子的用戶。

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.1
- 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。

2024/07/01

macOS平臺出現Poseidon惡意竊密程式

Poseidon 是一種針對 macOS 平臺的全新惡意竊密程式。該惡意軟體由原有的 RodStealer 惡意竊密程式演化而來。Poseidon 的程式碼和功能與另一個熱門的 macOS 惡意軟體變種 AMOS Stealer 非常相似。惡意竊密程式允許攻擊者進行檔案擷取、加密貨幣錢包竊取、收集儲存在網路瀏覽器中的資料以及遭入侵端點上密碼管理器中的資料。據觀察，Poseidon 惡意竊密程式是透過惡意 Google 廣告傳播，惡意軟體偽裝成 macOS 的 Arc 網頁瀏覽器之安裝程式。

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：

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：

- OSX.Trojan.Gen
- 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。

2024/07/01

老舊漏洞CVE-2021-40444，被開採濫用來傳遞MerkSpy惡意軟體有效酬載

Fortinet 研究人員揭露一個傳播 MerkSpy 惡意軟體的新行動。該行動幕後的主使者一直在開採濫用幾年前就已接露的微軟 MSHTML RCE 漏洞 (CVE-2021-40444) 傳播有效酬載。MerkSpy 是一種間諜軟體後繼變種，能夠監控使用者活動、螢幕截圖、鍵盤測錄、收集機密資料並將其洩露給攻擊者等。據報導，此次觀察到的惡意軟體傳播行動主要針對北美和印度。

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-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- 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
- Trojan.Gen.NPE.C
- Trojan.Mdropper
- Web.Reputation.1

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：

- Web Attack: Microsoft MSHTML RCE CVE-2021-40444
- 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。

2024/06/30

Kematian惡意竊密程式

研究人員發表一種名為 Kematian 的全新惡意竊密程式。這種基於 PowerShell 的工具用於從 Windows 系統秘密存取和傳輸資料。該工具收集各種敏感資訊，例如：助字詞 (Seed Phrase)、對話檔、密碼、應用程式資料和 Discord 權杖。這些資料透過 TCP 安全地傳輸到專用的 C&C 伺服器，以便解密和進一步利用。

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：

自適應防護技術(包含於SESC)：

- ACM.Mshta-Http!g1
- ACM.Mshta-Ps!g1
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Ps-Net!g1
- ACM.Ps-Wscr!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：

- CL.Downloader!gen38
- ISB.Heuristic!gen51
- Trojan.Gen.NPE
- WS.Malware.1

2024/06/30

假冒伊拉克中央銀行的 ZainCash APP，正在竊取行動裝置用戶資料

ZainCash 是伊拉克中央銀行官方所提供的綜合行動錢包服務，主要在提供各種數位金融服務，但它已成為最近遭網路犯罪分子濫用的金融科技品牌之一。有人發現有駭客使用假冒的 ZainCash Android 應用程式 (ZainCash.apk) 引誘不同國家的行動用戶。

如果使用者被成功誘騙安裝該惡意 APP，一經執行就會連接到一個像極 ZainCash 的 C&C 網域。該惡意軟體能夠竊取簡訊、裝置資訊 (例如：製造商、型號等) 和連絡人資訊 (包括號碼和姓名)。竊取的資料會透過 Telegram 殭屍 API 轉移到駭客的 Telegram 頻道。

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

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。

2024/06/28

Unfurling Hemlock：為多種惡意軟體感染部署惡意軟體集束炸彈

被稱為 Unfurling Hemlock 的駭客組織採用一種被稱為『惡意軟體集束炸彈』的方法，用多個惡意軟體同時感染目標系統。這種方法使威脅者能夠傳播更多惡意軟體，主要包括 Redline、RisePro 和 Mystic Stealer 等惡意竊密程式，以及 Amadey 和 SmokeLoader 等惡意載入器。這些惡意工具一旦安裝到目標系統上，就會被用來竊取敏感資訊，並可用做其進一步的非法活動。

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-RgPst!g1
- ACM.Untrst-Schtsk!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh.C!gen13
- SONAR.SuspBeh!gen736
- SONAR.ProcHijack!g45

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
- WS.Malware.1

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

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。

2024/06/28

Latrodectus惡意軟體行動：利用Firebase類型的網頁和遠端存取伎倆進行網路釣魚

Latrodectus 是一種熱門的惡意程式載入器，駭客圈利用它下載有效酬載並執行任意命令。網路釣魚郵件是傳播 Latrodectus 最常見的攻擊媒介。

最近，發現一個利用 Firebase 類型網頁呼叫 JavaScript 檔案的網路攻擊行動。啟動 JavaScript 檔案後，它會自動取得安裝程式並執行 Latrodectus。安裝完成後，Latrodectus 惡意軟體會與其命令控制 (C&C) 伺服器建立連線，讓惡意行為者遠端存取遭感染的裝置。此外，該惡意軟體還具有反虛擬機器和反偵錯功能，並建立一個排程以達到常駐的功能。

網路知識：Firebase 是 Google 的行動應用程式開發平台。其優勢包括端對端開發環境、更快的上市時間、建立應用程式和可擴展的基礎架構。Firebase 是建置 Web 與行動應用程式的後端平台。

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-Wscr!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。

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：

- ISB.Downloader!gen195
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Web.Reputation.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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: Scripting Host Processes Making Network Connections

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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片）軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。