保安資訊--本周(台灣時間2024/08/30)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 48 萬 3,600 台受保護端點上總共阻止了 4,940 萬次攻擊。這些攻擊中有 81.5% 在感染階段前就被有效阻止：**(2024/08/26)**

- 在**9**萬台端點上，阻止了**1,200**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11**萬**6,800**台端點上，阻止了**920**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3**萬**2,100**台**Windows**伺服主機上，阻止了**78**萬次攻擊。
- 在**5**萬**4,300**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**1,100**台端點上，阻止了**70**萬**8,300**次嘗試掃描在**CMS**漏洞。
- 在**4**萬**5,900**台端點上，阻止了**230**萬次嘗試利用的應用程式漏洞。
- 在**14**萬**2,900**台端點上，阻止了**590**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1**萬**6,700**台端點上，阻止了**120**萬次加密貨幣挖礦攻擊。
- 在**10**萬台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**641**台端點上，阻止了**8**萬**7,100**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 12 萬 8,300 個受保護端點上阻止了總計 350 萬次攻擊。**(2024/08/26)**

- 使用網頁信譽情資，在 **119.6K** 個端點上阻止 **310** 萬次攻擊。
- 攔截 **18.8K** 個端點上 **306.3K** 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 **7K** 個端點上攔截 **67.6K** 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 **215** 個端點上攔截 **6.3K** 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。

2024/08/29

Snake鍵盤側錄惡意程式出現全新變種

Fortinet 的研究人員提出 Snake 鍵盤側錄惡意程式出現全新變種的案例報告。此惡意軟體以惡意 .xls 附件的形式透過網路釣魚散佈。散佈 Excel 檔案包含針對舊版 WordPad RTF 漏洞 CVE-2017-0199 的開採濫用攻擊。攻擊者還在此行動的攻擊鏈中利用 .hta 檔案、VBscript 和 PowerShell 程式碼。Snake 鍵盤側錄惡意程式是一款基於 .NET 的惡意竊密程式，能夠竊取各種機密資料，包括系統資訊、憑證、按鍵、剪貼簿……等。收集到的資料會透過 SMTP 郵件通訊協定傳送回攻擊者。

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.SuspBeh!gen752

SONAR.SuspLaunch!g310

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：

- CL.Downloader!gen12
- CL.Suspexec!gen8
- ISB.Downloader!gen80
- ISB.Houdini!gen6
- MSIL.Packed.43
- Scr.Malcode!gdn34
- Scr.Malcode!gen59
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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

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: Malicious RTF File CVE-2017-0199

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。

2024/08/29

「Angry Stealer」惡意竊密程式攻擊行動，採用進階的惡意程式植入器並透過Telegram頻道來散佈

一個進階的惡意程式植入器程式檔已被識別，是設計用來部署稱為「Angry Stealer」的惡意竊密程式，該程式在 Telegram 和其他線上平台大量的曝光。Angry Stealer 的目標是敏感資料，例如：瀏覽器資訊、加密貨幣錢包、VPN 認證和系統細節，並透過 Telegram 滲出這些資料。Angry Stealer 似乎是源於「Rage Stealer」，共用相同的程式碼和功能。該植入器會執行兩個有效酬載：主要的「Stepasha.exe」用於資料竊取，而次要的「MotherRussia.exe」可能會作為製作惡意可執行檔的建置工具。

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.Dropper
- SONAR.MalTraffic!gen1
- SONAR.Stealer!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.MBT
- WS.Malware.1
- WS.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
- 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。

2024/08/29

Godzilla webhell部署行動

據報導，在真實網路情境上新發現部署 Godzilla webshell 的攻擊行動。攻擊者目標是有運行 ASP.NET 機器的組織，這些機器具有易受攻擊的環境設定，並利用 ViewState 功能將惡意 webshell 發佈到受害者的環境中。Godzilla webshell 以 .jar 檔案的形式傳送，用來執行遠端指令或 shellcode，並下載額外的有效酬載。

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-RunSys!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：

- Backdoor.Trojan
- Hacktool
- Hacktool.Jsprat
- Hacktool.Webshell
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- WS.Malware.1
- WS.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。

2024/08/29

以北約為主題的惡意軟體攻擊，鎖定捷克共和國官員

據報導，捷克共和國發生針對政府和軍方官員的惡意軟體攻擊行動。此行動背後的威脅發動者據信來自俄羅斯，並重度使用開放原始碼攻擊工具。為了引誘受害者，他們使用以北約為主題的誘餌檔案，並部署多階段攻擊鏈，其中包括惡意批次腳本、基於 Rust 的惡意程式載入器，以及及後滲透 C2 框架 (例如：Havoc、Sliver 和 Freeze)。為了躲避偵測並維持遭入侵系統的常駐能力，他們使用包括 ETW 修補程式、程序注入和加密有效酬載等先進技術。

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。

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：

- Backdoor.Cobalt
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Malware.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

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。

2024/08/28

高風險等級的CVE-2023-22527漏洞，已遭開採濫用於進行加密挖礦

根據報告，CVE-2023-22527 這個高風險等級的漏洞已在真實網路情境上被大肆開採濫用。此漏洞是存在 Atlassian Confluence Data Center 和 Server 中的嚴重 OGNL 注入漏洞。威脅者正利用此漏洞進行挖礦劫持，將受攻擊的系統轉變為加密挖礦網路。攻擊媒介／手法包括部署 shell 腳本和植入 XMRig 挖礦程式，同時透過 cron 工具的定期自動化功能以維持常駐能力。

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：

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
- 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: Atlassian Confluence RCE CVE-2023-22527

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。

2024/08/28

大選就是釣魚祭～針對美國選民發動的網路釣魚行動

美國總統大選距離現在只有短短幾個月，有媒體報導指稱有網路入侵事件意圖影響競選活動。我們審查 2024 年 5 月 1 日至 8 月 12 日期間註冊的新網域名稱，其中包含『harris』、『walz』或『trump』這些網域名稱。由於『vance』這個字串出現在許多英文單詞和與選舉無關的網域名稱中，我們排除包含該字串的網域名稱。我們的研究發現 216 個具有網路釣魚行為的網域名稱，以及 66 個上架惡意內容的網域名稱，這些很可能與民主黨或共和黨候選人有關。

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。

2024/08/28

手機／行動平台惡意軟體：Rocinante

Rocinante 是一種常見於針對巴西的手機／行動平台惡意軟體。就功能而言，Rocinante 有能力透過鍵盤側錄竊取資訊、啟動遠端存取連線、模擬受感染裝置上的拖曳和滑動動作或觸控手勢。惡意軟體也可能被利用來進行網路釣魚攻擊，顯示偽造的登入網站，進而竊取銀行憑證。Rocinante 可透過 HTTP 通訊協定或 Web Sockets 與攻擊者的基礎架構進行通訊，並將收集到的資料外洩。

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
- AppRisk:Generisk

2024/08/28

新興惡意程式載入器：Emmental偽裝成二進位檔案大肆散播

自 2024 年 2 月起，已偵測到一種名為 Emmental 的惡意程式載入器常常涉入資安事件，並透過偽裝的 Windows 二進位檔中散佈。此惡意程式載入器採用 HTA 檔案，並利用傳統的電子郵件釣魚手法，包括偽造影片，以全球各地的組織為目標。它已經成為全球數個使用 Bunny.net CDN 供應商和 WebDAV 伺服器散佈各種惡意軟體有效酬載行動的一部分，例如：CryptBot、AsyncRAT、Lumma、Meduza stealer、Xworm 和 SectopRAT。此工具的功能與地下市場所宣傳的功能差不多。

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.AdInPr-Lnch!g1
- ACM.Mshta-Ps!g1
- ACM.Rgsvc-Lnch!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g221
- 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。

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：

- CL.Downloader!gen55
- CL.Downloader!gen234
- Scr.Malcode!gdn14
- Scr.Malcode!gen
- Scr.Malcode!gen43
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malscript
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.B!300
- 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。

2024/08/27
防護亮點：賽門鐵克檔案信譽系統

賽門鐵克檔案信譽系統

賽門鐵克檔案信譽系統 (Symantec File Reputation System) 是賽門鐵克領先業界防護功能的基石。檔案信譽資料庫維護超過 80 億個檔案的信任與惡意程度的評等。它每天處理超過 2,000 萬項新的信譽變更，讓每天有超過 400 萬個新檔案和簽章者新增至檔案信譽資料庫。維護所有檔案的即時信譽資料庫的優勢之一，就是可以快速偵測到進入到客戶網路的新惡意軟體，而不會有中斷業務運作的風險。

基於「信譽」惡意軟體偵測所面臨的挑戰，是某些用於識別惡意軟體的標記可能與賽門鐵克客戶開發和部署的自建應用程式的標記非常相似。這些標記可能包括以下項目：

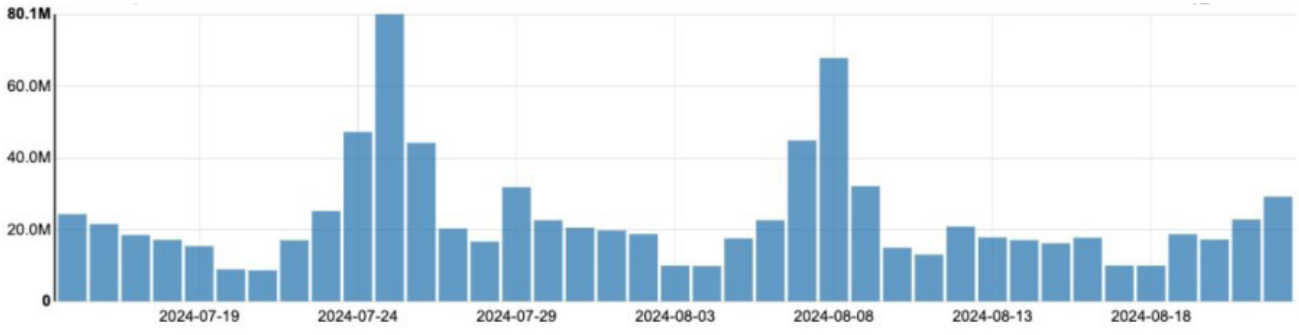
- 檔案在我們的使用者社群中並不普遍
- 檔案並非由可信賴的權威機構簽署
- 檔案會隨著新更新的推出而經常變更
- 檔案經常被混淆
- 檔案以多步驟安裝程式安裝，看起來像是多階段的惡意軟體攻擊

適用於各種情境是關鍵

為了成功攔截惡意軟體且不干擾業務運作，賽門鐵克檔案信譽系統會適應客戶的環境，並學習如何區分自行開發的應用程式與惡意軟體，即使許多跡象與上述相似。這些技術包括：

- 主動型白名單計畫 (Proactive Allow Listing Program)：可信賴的客戶可以註冊賽門鐵克主動允許清單程式，並提交自訂應用程式。
- 相似性分析 (Similarity Analysis) 以識別應用程式的更新：這包括根據相似度指標對檔案進行集結，並識別自行開發的應用程式的更新。
- 簽章信譽的可調適性 (Adaptive Signer Reputation)：賽門鐵克可辨識對您的組織而言是特定的簽章，並追蹤為「允許」的簽章者。
- 應用程式安裝標記：賽門鐵克使用啟發式方法來識別應用程式的安裝方式，這可能包括檔案安裝的位置、檔案與其他檔案的結合方式、檔案在您組織中時間、用於散佈檔案的 IP 位址等。

下圖顯示的是被過濾封鎖的自建應用程式「信譽」查詢數量。這個高效率的評級系統對於賽門鐵克的低誤報率 (FP) 貢獻良多。



欲深入瞭解「下載防護：下載鑑識」的詳細資訊，請點擊此處。
欲深入瞭解有關 Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策，請點擊此處。

2024/08/27
HZ RAT端存取木馬出現macOS平台上的版本

macOS 平台上的全新：HZ RAT 端存取木馬在真實網路情境上出現。根據最近的報導，該惡意軟體的目標是企業通訊工具 DingTalk 和訊息平台 WeChat 的使用者。該惡意軟體具有一些基本功能，可以收集受感染機器的資訊、微信和 DingTalk 應用程式中的用戶資訊，以及存儲在 Google Password Manager 中的用戶資料等。收集到的資訊會傳回攻擊者控制的 C&C 伺服器，並可能用於日後的攻擊。

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。

2024/08/27
針對亞太地區使用者的網路釣魚行動

賽門鐵克最近發現一個針對亞太地區使用者的網路釣魚行動。此網路釣魚活動濫用 HTML 檔案，將非法取得的憑證發佈至第三方託管服務，在此案例中為 nocodeform[.]io。這些訊息會以「postmaster」或「MAILER-DAEMON」的郵件位址名稱傳送，藉此隱藏自己。

主旨範例：

- 您已收到新的 51 電子发票【发票号：67479463】
- Non remis : New Fineline Retailer Purchase Orders Have Arrived!!*新的 Fineline 零售商採購訂單已收到!

範例檔案名稱：

- QUOTE_3636.html
- PO-#0094321.html
- new order.htm
- Shipment.docs.html

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：

- Phish.ScptML.B
- Phish.ScrHtml!gen8
- Phishing.HTM.Gen

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。

2024/08/27

網路釣魚行動以可縮放向量圖形(SVG)攻擊拉丁美洲和加勒比海地區產業的電子郵件憑證

在八月初，賽門鐵克觀察到一個攻擊者以拉丁美洲的多家公司為目標，包含零售、法律、乳製品、金融、能源和汽車製造等行業。其目的是收集電子郵件憑證，這些憑證在販賣初始存取的仲介市場非常強手，並助長進一步的入侵，包括財務竊取、網路間諜和勒索軟體攻擊。

該電子郵件 (主旨：Orden de compra a Brasil - [目標公司的縮寫]) 似乎是冒充一家名為 Expansão BR 公司所發出的採購洽詢，該公司在巴西從事進口業務。寄件人表示有興趣向收件人的公司購買產品，並詢問運送至巴西的事宜。該電子郵件包含一個惡意 SVG 檔案 (LISTA DE ORDENES DE COMPRA__PDF.svg) 的附件採購訂單，並要求正式確認，以及運送方式和預計運送時間的詳細資訊。開啟 SVG 檔案後，會顯示偽造的 Microsoft 登入頁面，如果使用者輸入憑證，就會傳送至攻擊者操控的惡意站台。

使用可縮放向量圖形 (SVG：Scalable Vector Graphics) 並不是新鮮事，但在電子郵件威脅中已有越來越多人觀察到它被用來進行不同規模和目標族群的網路釣魚攻擊。雖然許多使用者都熟悉 HTML，但在電子郵件中使用 SVG 檔案可能更具欺騙性，因為 SVG 檔案較不為人所知，讓攻擊者得以利用這種不熟悉的情況。

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：

- Phish.Gen

2024/08/27

傳播Cheana惡意竊密程式的網路釣魚行動：鎖定VPN使用者

據報導，有威脅者鎖定下載 VPN 軟體的使用者進行網路釣魚行動。偽裝成 WarpVPN 原廠的釣魚網站會散佈不同作業系統平台的惡意竊密程式。該惡意軟體被稱為 Cheana ，會收集和滲出各種類型的資訊，例如：瀏覽器內儲存的資料、cookie、密碼、加密貨幣錢包和加密貨幣瀏覽器擴展。Linux 和 macOS 版本具有竊取 SSH 金鑰和 Keychain 資料的特定功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-CPE!g2
- ACM.Ps-Http!g2
- 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：

- OSX.Trojan.Gen
- 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。

2024/08/26

Dolphin Loader惡意程式載入器：濫用遠端監控與管理(RMM)工具的全新惡意軟體即服務威脅

Dolphin Loader 是一種新的惡意軟體即服務 (MaaS) 惡意程式載入器，於 2024 年 7 月首次被觀察到在 Telegram 上出售。它被用來散佈各種惡意軟體有效酬載，例如：SectopRAT、LummaC2 和 Redline，主要是透過隨意下載的方式散佈。該惡意程式載入器利用遠端監控與管理 (RMM：Remote Monitoring and Management) 工具的功能，例如：遠端指令執行與系統監控，來隱蔽操作並避免偵測。其技倆包括濫用 AutoIt 腳本來執行有效酬載，以及濫用 ITarian RMM 軟體傳送惡意內容。RMM 軟體是 IT 部門和管理服務供應商 (MSP) 用來遠端監控和管理其網路及 IT 資產的一種軟體工具或平台。此外，Dolphin Loader 利用延伸驗證 (EV) 憑證繞過 SmartScreen、避開 Chrome 瀏覽器的安全警示，並避免被端點偵測與回應 (EDR) 系統偵測到。

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：

- Scr.Malcode!gen
- Trojan Horse
- 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。

2024/08/26

攻擊者操弄遭入侵的網站散播惡意軟體

研究人員發現，惡意軟體會在遭入侵的網站上偽裝成瀏覽器更新進行傳播。當使用者瀏覽這些網站時，會被提示引誘下載偽裝成 Chrome 或 Firefox 瀏覽器更新的惡意檔案。這些檔案可以是 EXE、ZIP、APPX 或 VHD 等各種格式。VHD 檔案包含隱藏的捷徑 (LNK)，可執行 PowerShell 指令並連線至攻擊者操控的 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：

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：

- Scr.Mallnk!gen13
- Scr.Malcode!gen43
- 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。

2024/08/26

潛伏在南非冒充兩家主要銀行的APP，SpyNote手機惡意軟體蠢蠢欲動

賽門鐵克最近在南非的手機／行動裝置威脅領域發現 ，安卓平台上遠端存取木馬：SpyNote 的後繼新變種。一名威脅份子假冒兩家主要金融機構 Nedbank 和 Absa，企圖引誘使用者在裝置上安裝惡意 APP，導致未經授權交易、身分盜用和敏感個人資訊外洩等財務損失。

目前，感染途徑與手法仍未確認，但惡意APP的安裝套件檔 (「Absa Bank en.apk」、「ABSA

BANK.apk」和「Ned Bank.apk」) 極有可能是透過簡訊散發，其中包含虛假銀行 APP 所誘導的惡意網址--這是這類電子犯罪行為者的經典且普遍的手法。

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：

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

2024/08/25

Cthulhu惡意竊密程式鎖定macOS用戶電子錢包、帳號密碼而來

研究人員最近觀察到另一種針對 MacOS 使用者的惡意軟體即服務 (MaaS)，稱為 Cthulhu。此惡意軟體以蘋果磁碟映像 (DMG) 形式形式傳送，其中包含特定平台的二進位檔案，並以 GoLang 開發。它會偽裝成合法軟體，誘騙使用者開啟 DMG，然後使用 macOS 的「osascript」工具來提示輸入密碼，並取得未經授權的存取權。

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
- OSX.Trojan.Gen.2
- 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。

2024/08/23

Peaklight惡意下載程式涉入惡意軟體活動的報告

Peaklight 是 Mandiant 研究人員發現一種全新 PowerShell 類型的惡意下載程式。該惡意軟體已被用於最近的攻擊行動中，散佈各種有效酬載，包括 Lumma 惡意竊密程式、ShadowLadder 和 CryptBot。攻擊者利用偽裝成影片檔的惡意 .lnk 檔案，以及多階段攻擊鏈中的 JavaScript 載入程式。Peaklight 下載程式的主要功能是從遠端 CDN (內容傳輸網路) 網站擷取 .zip 壓縮有效載荷，提取後並在受感染的機器上執行。

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：

自適應防護技術(包含於SESC)：

- ACM.Mshta-Http!g1
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper!gen2
- SONAR.SuspPE!gen32
- 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：

- CL.Downloader!gen111
- Downloader
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.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
- 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：

- 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。

2024/08/23

CVE-2024-4885--網路監控系統WhatsUp Gold的遠端程式碼漏洞(RCE)

CVE-2024-4885 是最近揭露嚴重等級 (CVSS 風險評分：9.8 分) 未經驗證的遠端程式碼漏洞，會影響網路監控系統 WhatsUp Gold。利用此漏洞，未經驗證的攻擊者可能會以 iisapppool／nmconsole 權限執行任意指令。雖然該漏洞已被報導在真實網路情境上被大肆開採濫用，但原廠已釋出修補程式 2023.1.3 版本的軟體來解決該漏洞。

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: Progress WhatsUpGold CVE-2024-4885

2024/08/23

Sedexp：使用udev規則來取得長駐能力的Linux惡意軟體

Sedexp 是最近發現會影響 Linux 環境的威脅。據報告，Sedexp 惡意軟體利用 udev 規則來建立在受感染機器的長駐能力。Udev 是 Linux 上的裝置管理系統，可管理 /dev 目錄中的裝置節點。特定的 udev 規則會定義要採取動作或載入的驅動程式，例如：當有新的裝置連接時。Sedexp 惡意軟體允許反向 shell 執行，讓威脅者能夠控制受感染的端點。

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：

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.Trojan

2024/08/23

PG_MEM--針對PostgreSQL伺服器進行加密挖礦的惡意軟體

PG_MEM 是最近在真實網路情境上觀察到的全新惡意軟體。散佈此惡意軟體的攻擊行動利用暴力攻擊脆弱的 PostgreSQL 資料庫伺服器。一旦攻擊者取得伺服器的存取權限，便會嘗試透過建立新的高權限帳戶來建立長駐能力。之後，威脅者會啟動系統搜尋，並傳送 PG_MEM 植入器的有效載荷，最終將 XMRig 挖礦程式傳送至受感染的機器。

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：

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：

- LLinux.Coinminer
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.3

2024/08/22

CMoon：在俄羅斯天然氣行業裡流竄 .NET 型態的惡意程式蠕蟲

CMoon 是一種以 .NET 為基礎的惡意程式蠕蟲，在俄羅斯一家受攻擊的氣化與瓦斯供應公司的網站上被發現。此惡意軟體偽裝成合法的法規文件，並以惡意執行檔的連結取代各種網站連結。該蠕蟲具有擷取螢幕截圖、收集敏感資料、進行 DDoS 攻擊，以及與指揮與控制 (C&C) 伺服器建立連線以接收指令和下載其他惡意有效酬載的能力。

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：

自適應防護技術(包含於SESC)：

- ACM.Untrst-FlPst!g1
- ACM.Untrst-RunSys!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：

- Infostealer
- WS.Malware.1

基於機器學習的防禦技術：

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

2024/08/22

冒充沙迦的港務局的目標式網路釣魚行動，散播Casbaneiro惡意程式

在網路安全方面，由於港口和相關機關在全球供應鏈中扮演不可或缺的角色，並與運輸、物流、能源和政府部門等產業相關聯，因此成為威脅者的高價值目標。詐騙者經常偽裝成港務局，引誘其他產業進行網路釣魚詐騙或社交工程攻擊。

賽門鐵克最近觀察到一個魚叉式／目標式網路釣魚行動，有攻擊者假冒沙迦港務局 (Sharjah Ports Authority) 的員工，以阿拉伯聯合大公國 (UAE) 的能源公司為目標。沙迦港 (Port Khalid) 是阿拉伯聯合大公國 (UAE) 沙迦的主要海運樞紐，處理多樣化的貨物，並支援當地工業與全球的聯繫。

該電子郵件 (主旨：DOCUMENTS AS REQUESTED) 包含一個惡意的 .RAR 壓縮檔 (Documents SPA-H24029629800 details.rar)，裡面有多個檔案，其中包括一份偽造的買賣協議 (Documents SPA-H24029629800 details.exe)，這是一份被改過檔名的合法檔案「rmiregistry.exe」。當執行該檔案時，它會側載一個惡意 DLL「jli.dll」，並透過一個名為 Casbaneiro 的銀行惡意軟體入侵機器。

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：

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。

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：

- Trojan.Casbaneiro

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**。