保安資訊--本周(台灣時間2024/08/02)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 4,200 台受保護端點上總共阻止了 4,650 萬次攻擊。這些攻擊中有 80.4% 在感染階段前就被有效阻止：**(2024/07/29)**

- 在**9萬3,100**台端點上，阻止了**1,180**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬5,500**台端點上，阻止了**910**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬3,100**台**Windows**伺服主機上，阻止了**79**萬次攻擊。
- 在**5萬7,300**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬800**台端點上，阻止了**65萬5,100**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,300**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**15萬3,700**台端點上，阻止了**370**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,100**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬7,100**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**708**台端點上，阻止了**9萬4,100**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 10 萬 6,500 個受保護端點上阻止了總計 330 萬次攻擊。**(2024/07/29)**

- 使用網頁信譽情資，在 **98K** 個端點上阻止 **290** 萬次攻擊。
- 攔截 **19.2K** 個端點上 **346.7K** 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 **6K** 個端點上攔截 **65.8K** 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 **212** 個端點上攔截 **6.7K** 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。

2024/08/02

APT駭客集團：Bloody Wolf大肆散播STRRAT惡意軟體

據報導，被稱為 Bloody Wolf 的 APT 駭客集團針對哈薩克共和國的組織發動惡意軟體攻擊行動。該駭客集團發送仿冒哈薩克共和國財政部及其他機構的網路釣魚電子郵件。這些電子郵件包含 PDF 附件內嵌 JAR 檔案的下載連結，而下載 JAR 檔案實際上是惡意的 STRRAT 惡意軟體。STRRAT 具備系統資訊收集、鍵盤側錄、瀏覽器資料收集等功能，然後將資料滲出到攻擊者操控的 C&C 伺服器。此外，它還能啟用遠端連線，讓攻擊者下載並執行其他惡意軟體或指令。

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：

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：

- Java.Strrat
- Trojan.Maljava
- WS.Malware.1
- WS.SecurityRisk.4

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。

2024/08/01

Mandrake手機／行動裝置平台上的間諜軟體

Mandrake 手機／行動平台上間諜軟體的最新變種已透過 Google Play 商店上的多個 APP 散佈。其中最早的 APP 稱為 AirFS，早在 2022 年就首次上架到 Google Play 商店，直到今年 3 月仍可供下載。該惡意軟體具有收集使用者資料、執行遠端指令、擷取螢幕或安裝其他 APP 的功能。這個最新 Mandrake 變種具有新的混淆層以及多種已實作的反分析與迴避技術。

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：

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
- Android.Reputation.2
- 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。

2024/08/01

TgRAT惡意軟體以Linux的變種強勢回歸

TgRAT 是早在 2022 年就被發現的惡意軟體 (歸類為遠端存取木馬：RAT)，最初以 Windows 系統為攻擊目標。本月初，此 RAT 的 Linux 版本被發現在真實網路情境大肆散佈。感染目標機器後，惡意軟體會執行任意指令／指令碼、收集螢幕截圖或從受攻擊的主機中擷取使用者檔案。攻擊者透過 Telegram 機器人 (Telegram Bot) 來控制 TgRAT。

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.NPE
- WS.Malware.1

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，DCS 可防止 TgRAT 惡意軟體的安裝和惡意活動，提供零時差保護。
- DCS 出廠就內建的強化政策，可防止惡意軟體在系統上植入或執行。
- DCS 出廠就內建的強化政策，可以保護 Linux 伺服器防止從暫存檔案或其他可寫入位置執行惡意軟體，這是惡意軟體中使用的一種技術。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/31

安卓平台上的勒索軟體：SARA以假冒的APP騙局來瞄準越南行動用戶

安卓平台上的裝置鎖定惡意程式 (Lockers) 和勒索軟體在幾年前非常盛行，尤其是在 RansomLock 熱潮期間。如今，雖然它們仍然存在於行動威脅中，但其普遍性已經降低。這些威脅通常會將使用者鎖定在其裝置之外，並顯示贖金訊息，要求支付解鎖碼以重新取得存取權。這些威脅有許多變種，但其中一種具有螢幕鎖定和檔案加密功能的特殊變種 SARA 似乎已頗受歡迎。

在最近案例中，賽門鐵克在越南觀察到 SARA 偽裝成虛假 MB Bank(軍事商業股份銀行) 安卓平台上的 APP，以行動裝置使用者為目標。目前尚不清楚這些 APP 的傳播方式，但很可能是透過附有惡意網址的簡訊傳播。其中一個 APP 寄存在線上檔案傳輸與分享工具 UpFile。

在過去一年中，有更多 SARA 涉入的案例已經出現，多個行動者將此駭客軟體偽裝成虛假的 Spotify、CashApp、Instagram、優惠券 APP、YouTube、Chrome 更新、遊戲等。

執行後，SARA 會要求各種權限，例如：存取檔案與媒體、聯絡人、簡訊和位置。然後，它會根據行動者的設定，鎖定螢幕或加密受害者裝置上的檔案。如果是後者，它會產生加密密碼，並將其儲存至共用偏好設定。然後，它會嘗試加密檔案 (txt、jpg、jpeg、pdf、zip、doc、xls 等)，並附加 .enc 副檔名。接下來，它會產生檔案以儲存用於加密的鹽值和 IV (初始化向量) 值。最後，它會在目錄中投放贖金支付說明文字檔 (README.txt)，並發送標題為 「Locked 」的通知，其中文字說明檔案已被加密，並請您閱讀贖金支付說明。

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

2024/07/31

DeerStealer惡意軟體透過假冒的Google身分驗證器(Google Authenticator)網站散佈

在真實網路情境上發現一起全新的惡意行動，散佈 DeerStealer 惡意竊密軟體。該惡意軟體以偽造的 Google 身分驗證器 (Google Authenticator)APP 為幌子進行散佈，惡意二進位檔上架在 Github 儲存庫中。該惡意軟體以 Delphi 程式語言編寫，從受攻擊的端點收集機密資料，並將竊取的資料以 PKZIP 檔案形式外洩至攻擊者控制的 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：

- 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.A!500
- 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。

2024/07/31

安卓平台上大規模的SMS Stealer惡意軟體散佈行動

據報導，一個持續進行的大規模行動，散佈一個名為 SMS Stealer 安卓平台上的惡意軟體，感染全球各地的行動裝置。此行動至少從 2022 年就開始活躍，目標受害者遍及 113 個國家。SMS Stealer 惡意軟體主要透過惡意廣告和 Telegram 殭屍散佈，受害者通常會被引導至模仿 Google Play 商店的惡意網頁。此惡意軟體具備多種資料竊取功能，主要集中於簡訊內容和雙重認證 (2FA) 的一次性密碼 (OTP) 竊取。利用此惡意軟體竊取的資料，可能會協助攻擊者進行進一步的詐欺活動或網路釣魚攻擊行動。

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：

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
- Android.Reputation.1
- Android.Reputation.2
- 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。

2024/07/31

ModiLoader惡意軟體載入器涉入針對波蘭中小型企業(SMB)的網路攻擊行動

Modiloader (也稱為DBatLoader) 惡意軟體載入器最近在波蘭、義大利和羅馬尼亞的中小型企業 (SMB) 攻擊行動中被部署。Modiloader 透過各種檔案格式的惡意電子郵件附件傳播，例如：.img、.tar、.rar 或 .iso。Modiloader 是基於 Delphi 的惡意軟體，用於下載和執行傳送到受攻擊機器的最終有效酬載。有效酬載通常各不相同，已知的攻擊行動一直在執行 Agent Tesla、Remcos 或 Formbook 系列的惡意軟體。

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：

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.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.Suspexec!gen168
- Scr.Malcode!gen43
- Scr.Malscript!gen1
- Trojan Horse
- Trojan.Formbook

- Trojan.Gen.MBT
- WS.Malware.1
- 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!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：

- 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。

2024/07/30

DoNot APT駭客組織以巴基斯坦安卓手機使用者為目標

APT-C-35 (也稱為 DoNot APT 駭客組織) 至少從 2013 年開始就不斷涉入許多網路攻擊活動。最近，他們將目標對準巴基斯坦的安卓手機使用者。他們的攻擊通常從網路釣魚行動開始，進而部署稱為 StealJob 的安卓平台惡意軟體。這些威脅份子的主要目的是存取機密資訊和智慧財產。他們的技術包括加密和無檔案惡意軟體，以逃避偵測。

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.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

- 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。

2024/07/30
防護亮點：勒索軟體即服務(Ransomware-as-a-Service)的演進、影響以及緩解措施

浪頭上的 Eldorado：長江後浪催前浪，一代新人換舊人--勒索軟體即服務 (RaaS) 興起的這 12 年的寫照

威脅環境中惡意軟體之演進是網路安全專家無法安枕無憂的唯一原因，勒索軟體即服務 (RaaS) 的崛起與演化更是不遑多讓。從 2012 年首次出現的 Reveton，到最近 Eldorado 勒索軟體的出現，早期事件據稱每月賺取 40 萬美元，到現今資料外洩的成本超過 100 萬美元，有時甚至遠遠超過這個數字。本公報將簡單探討此趨勢，以及賽門鐵克的調適型防護 (Adaptive Security Protection) 如何幫助企業降低與 RaaS 攻擊鏈相關的風險。

認識勒索軟體即服務 (RaaS) 的攻擊鏈

勒索軟體集團非常依賴「就地取材」(LOTL：living-off-the-land) 戰術來運行其攻擊鏈的自動化，意即他們使用已遭感染系統上已有的現成工具。舉例來說，網路釣魚行動可能會傳送一封電子郵件，其中包含一個含有巨集或腳本的 Office(word／excel…) 或 PDF 附件。巨集會執行 PowerShell 指令碼，而 PowerShell 指令碼則會下載工具並將其注入記憶體以避免被偵測。然後，它會執行偵查指令，以瞭解被攻擊的系統，包括使用者權限和網路存取。一旦取得存取權限，攻擊者就可以為所欲為，從竊取資料到部署勒索軟體。

Eldorado 與過往勒索軟體即服務 (RaaS) 的交集

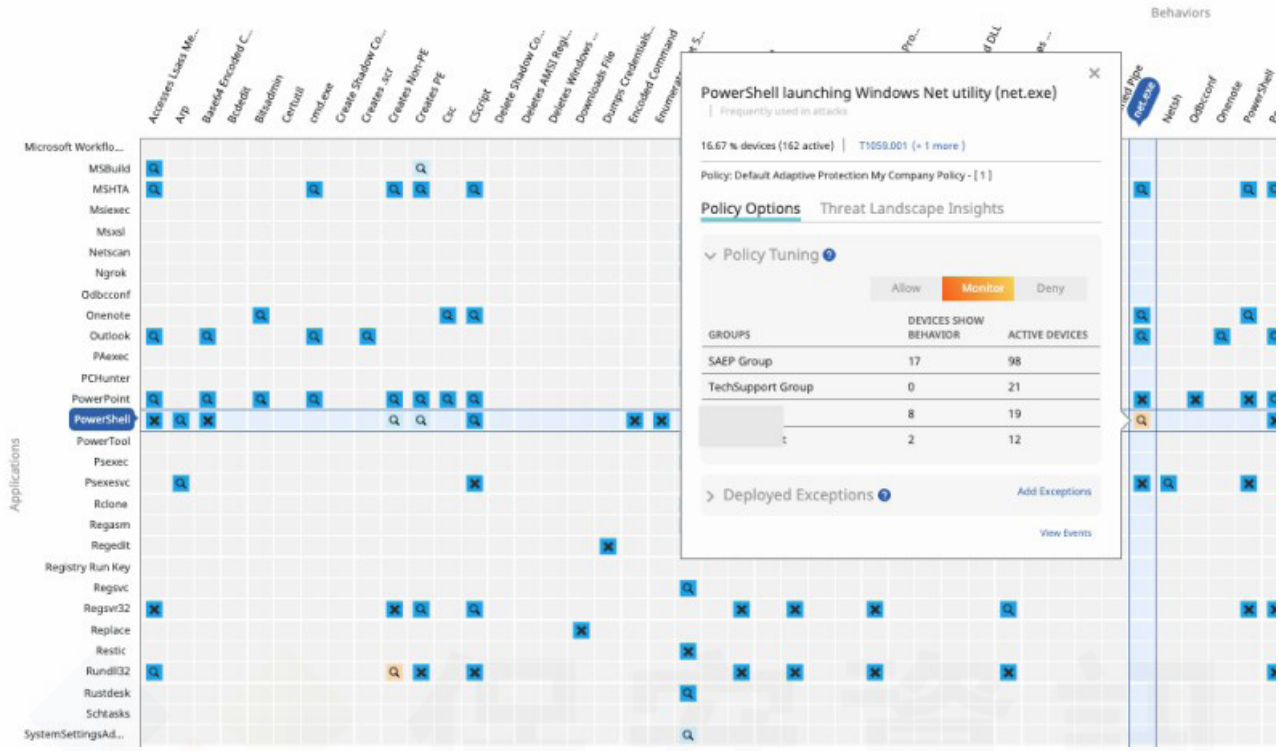
下表說明 Eldorado 與過去 RaaS 攻擊之間的交集，顯示使用共同的合法工具，例如：PowerShell、Scripts、WMI 和 Vssadmin。儘管威脅隨著時間演變，但工具和戰術仍保持一致。透過停用公司內不必要的應用程式行為，賽門鐵克的調適型防護 (Adaptive Security Protection) 可協助關閉攻擊者利用這些工具的大門，進而降低 LOTL 攻擊的風險。

下表列出了這些攻擊中發生的一些典型步驟：

行　為	Eldorado	Hive	LockBit
Word 下載／建立可執行或不可執行檔案	Y	Y	Y
Excel 下載／建立可執行或不可執行檔案	Y	N	N
PDF 下載／建立可執行或不可執行檔案	N	N	Y
Powershell 下載／建立可執行或不可執行檔案	Y	Y	Y
Powershell 執行網路指令	Y	Y	Y
Powershell 存取 http/https	N	Y	Y
Psexec／WMI 關閉安全軟體	Y	Y	Y
啟動 netscan 以掃描／診斷／調查／瞭解網路	N	Y	Y
Vssadmin 刪除磁碟區陰影複本	Y	Y	Y
使用 rclone.exe 竊取受害者資料	Y	N	Y

洞察力是改善防護的關鍵

以下 Adaptive Security 熱圖可深入瞭解組織內的行為使用情況，讓 IT 管理員可設定允許、監控或拒絕的行為。此外，它還可以建立例外情況，例如：一般將行為設定為拒絕，但在特定情況下則允許。



透過瞭解 RaaS 的演進並採用賽門鐵克的調適型防護 (Adaptive Security Protection)，企業可以更有效地防禦複雜的勒索軟體攻擊。停用不必要的工具和監控行為是降低 LOTL 戰術所造成風險的關鍵步驟。

欲深入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。
欲深入瞭解更多有關 Symantec Endpoint Security 中啟用調適型防護的資訊，請點擊此處。

2024/07/30

Leafperforator威脅組織涉入假冒巴基斯坦海洋事務部的文件，散播JavaScript惡意軟體的網路釣魚行動

據報導，Leafperforator (也稱為 SideWinder) 威脅組織利用強化的戰術和技術，發動全新惡意軟體攻擊行動。此威脅份子濫用魚叉式網路釣魚電子郵件，並以亞洲國家為目標。在最新的攻擊行動中，受害者會受到與裁員或減薪相關文件的誘騙，導致他們開啟偽裝的檔案。此檔案利用已知的安全漏洞 (CVE-2017-0199) 與偽裝成巴基斯坦港口與航運總局的惡意網站建立連絡。該網站隨後開採濫用 CVE-2017-11882 漏洞來擷取相關聯的 RTF 格式檔案，最終會導致 JavaScript 惡意軟體的傳送。

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：

- Bloodhound.RTF.12
- Bloodhound.RTF.20
- Scr.Malcode!gen
- Trojan.Gen.NPE
- Trojan.Mdropper
- WS.Malware.1

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。

2024/07/30

網路釣魚行動：惡意HTML附件模仿OneDrive以部署惡意軟體腳本

據報導，有新的網路釣魚行動使用模仿 Microsoft OneDrive 頁面的圖片檔案。釣魚活動是透過含有 HTML 附件的釣魚電子郵件誘騙受害者。開啟這些附件時，會顯示類似 OneDrive 頁面的影像，並顯示錯誤，表示 OneDrive 雲端服務出現連線問題。按一下提供「如何修復」按鈕，就會下載並擷取包含 AutoIt 腳本的壓縮檔。執行這些腳本會損害使用者的系統。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!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 Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- Scr.Malcode!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。

2024/07/30

UNC4393威脅組織最近涉入的活動

被稱為 UNC4393 的威脅組織至少從 2022 年起就活躍於威脅領域。該威脅組織已知會在攻擊中利用各種惡意軟體變種和客製化工具，包括 Basta 勒索軟體、KnotWrap 軟體程式、KnotRock 工具、DawnCry 軟體程式或 PortYard tunneler。2024 年觀察到這個威脅組織最近作業重點是部署 Basta 勒索軟體和資料竊取的雙重勒索。據報導，攻擊者也利用 SilentNight C/C++ 為基礎的後門，以惡意廣告的方式傳送。

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.SuspLaunch!g18
- SONAR.TCP!gen6

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.Basta
- Trojan.Gen.MBT
- WS.Malware.1

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.C

2024/07/30

Exela惡意竊密軟體繼續在真實網路情境散佈

Exela 是採用 Python 撰寫的全新惡意竊密軟體，去年才在威脅環境中被發現。最近幾週，在真實網路情境一直有發現散佈此惡意竊密軟體的網路攻擊行動。Exela 具有從受攻擊的機器收集和滲透多元資料之功能--這包括瀏覽器資料和 cookie、自動填寫資料、使用者憑證、會談檔案 (session files)、加密貨幣錢包和其他資料。惡意軟體利用 Discord 作為 C&C 通訊管道，並使用 Discord webhook 網址來進行資料外洩。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Mshta!g1
- ACM.Ps-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.SuspLoad!gen2
- 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：

- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- 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。

2024/07/30

Flame(*火焰)惡意竊密程式

全新的 Flame(*火焰) 惡意竊密程式是採用 C/C++ 撰寫，在 Discord 和 Telegram 上打廣告出售。該惡意軟體具有收集和滲出遭感染機器的各種資訊、Discord tokens、剪貼簿資料、憑證、銀行資訊和瀏覽器 cookies 等的功能。Flame 惡意竊密程式利用 Discord webhooks 來滲透所收集的資料。該惡意軟體使用 DLL 側載技術執行有效籌載，具有確保在受感染端點上常駐的功能，並會執行額外檢查以確定是否存在虛擬化或沙箱環境。

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-Mshta!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

2024/07/29

Hive0137威脅組織在最近的攻擊中採用大型語言模型(LLM) AI

被稱為 Hive0137 的威脅份子在最近的攻擊行動中採用大型語言模型 (LLM) 的 AI。LLM 是一種生成式人工智慧 (AI)，可以辨識和產生文字以及完成其他任務。Hive0137 威脅組織以惡意軟體散佈攻擊而聞名，這些攻擊通常會導致勒索軟體感染。例如：Warmcookie 後門就是該組織散佈的惡意軟體之一。該組織一直在腳本和釣魚電子郵件開發中使用 LLM。此外，最近還發現另一個行動與 Hive0137 威脅組織的攻擊行動相似 (也使用 LLM)，以 X-Worm 有效酬載來鎖定義大利的使用者。

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.SuspOpen!gen11

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 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
- 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。

2024/07/29

開放原始碼版本控制軟體Bazaar存在：CVE-2024-40348目錄遍歷漏洞

CVE-2024-40348 是一個最近揭露的目錄遍歷漏洞，影響開放原始碼版本控制軟體 Bazaar(版本 1.4.3)。成功開採濫用此漏洞可讓未認證的攻擊者，在受影響的系統上執行目錄遍歷，導致未經授權存取系統目錄和敏感檔案。此類存取可進一步讓攻擊者以任意程式碼部署及執行的形式，進行更進一步的系統入侵。

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: Bazaar Directory Traversal Vulnerability CVE-2024-40348

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，DCS 預設會保護作業系統，防止重要檔案／資源被篡改。此外，客戶可以選擇為 Bazaar 建立自訂沙箱，以鎖定重要檔案／目錄的讀／寫存取權限。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/29

通訊軟體Telegram上的爆紅遊戲「Hamster Kombat」深受用戶歡迎，網路騙子製造騙人的惡意農場機器人工具

隨著通訊軟體 Telegram 上「Hamster Kombat」遊戲的爆紅，越來越多的騙子開始瞄準玩家。遊戲創造者承諾會推出新的加密貨幣，並提供可觀的獎勵，這吸引許多玩家。因此出現聲稱提供 Hamster Kombat 下載的虛假應用程式商店。網路騙子以 Windows 使用者為目標，利用聲稱提供 Hamster Kombat 農場機器人和自動點擊程式的工具，協助玩家在遊戲中獲利最大化。實際上，這些工具是 Lumma Stealer Cryptors 的各種變種。

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.Rgasm-Lnch!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspOpen!gen11

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Whispergate
- Trojan.Gen.MBT
- WS.Malware.1

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。

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

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。

2024/07/29
OceanSpy勒索軟體

有人在真實網路情境觀察到一個自稱為 OceanCorp 的勒索軟體駭客組織攻擊單一的機器實例。目前，根據其贖金支付說明文字檔的說明 (OceanCorp.txt)，這個駭客不會執行雙重勒索戰術，也就是說他們不會威脅洩露或出售資料。他們似乎只專注於加密檔案來勒索，要求 0.015 比特幣 (BTC)。一旦機器受到他們的勒索軟體 (OceanSpy) 攻擊，就會在加密檔案中冠上 .[random4characters] 副檔名。感染的途徑／媒介／手法仍不確定，但根據觀察到的活動中涉入檔案名稱，很有可能是透過惡意電子郵件散佈。

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-RLsass!g1
- ACM.Untrst-FlPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDrop!gen1
- SONAR.SuspBeh.C!gen18
- SONAR.SuspLaunch!g22
- SONAR.SuspLaunch!g266

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Ransom.Sorry

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。

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，DCS 預設的強化政策可針對此勒索軟體提供零時差保護。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/07/28
越南正在流行的安卓平台惡意行動：間諜軟體偽裝成越南科技及商業股份銀行(Techcombank)的APP

過去幾年來，全球各地的駭客團體和個體戶都在使用 SpyNote 這種熱門的安卓平台遠端存取木馬程式 (RAT)，而且其熱度沒有絲毫降溫的跡象。針對企業和消費者的電子犯罪和目標性攻擊行動每天都在發生。

在最近一個例子中，賽門鐵克觀察到有個惡意行動者將其 SpyNote 變種偽裝成越南科技及商業股份銀行 (Techcombank) (Vietnam Technological and Commercial Joint Stock Bank) 的安卓平台 APP，以越南的行動使用者為目標。該惡意應用程式 (Techcombank_v3.10.13.apk) 存放在 GitHub 上，GitHub 是一個流行的版本控制與協作平台。

網路罪犯濫用 GitHub 發佈惡意有效酬載的情況越來越嚴重。當惡意安卓 APP 上架在 GitHubusercontent 站台上，這表示二進位檔案是直接從 GitHub 儲存庫提供。他們很可能透過釣魚電子郵件、簡訊、社交媒體或其他管道分享惡意網址，誘騙使用者下載並安裝他們的惡意二進位檔案。

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

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**。