保安資訊--本周(台灣時間2024/09/13)
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 46 萬 9,400 台受保護端點上總共阻止了 4,960 萬次攻擊。這些攻擊中有 81.9% 在感染階段前就被有效阻止：**(2024/09/09)**

- 在**8萬7,200**台端點上，阻止了**1,300**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬700**台端點上，阻止了**900**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬1,000**台**Windows**伺服主機上，阻止了**7萬5,000**次攻擊。
- 在**5萬2,200**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,500**台端點上，阻止了**72萬3,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,800**台端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在**13萬2,000**台端點上，阻止了**500**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6萬**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬1,000**台端點上，阻止了**790**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**570**台端點上，阻止了**7萬2,200**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 8,900 個受保護端點上阻止了總計 330 萬次攻擊。**(2024/09/09)**

- 使用網頁信譽情資，在 **110.8K** 個端點上阻止 **300** 萬次攻擊。
- 攔截 **17.8K** 個端點上 **258.9K** 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 **69.2K** 個端點上攔截 **7K** 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 **233** 個端點上攔截 **7.2K** 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。

2024/09/12

BLX(也稱為XLABB)惡意竊密程式涉入的網路攻擊行動

BLX 也稱為 XLABB，是去年首次發現全新惡意竊密程式。在真實網路上已發現到此惡意竊密程式所涉入的新活動。BLX 是一種源於開放原始碼的惡意軟體，透過 Telegram 和其他平台大肆散布。從功能上來看，該惡意軟體能夠從受遭入侵的端點竊取機密資料，專注在包括憑證、瀏覽器中儲存的資訊、第三方應用程式帳戶、Discord tokens、加密貨幣錢包等。

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：

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
- Trojan Horse
- WS.Malware.1

2024/09/12

PlugX和BadIIS惡意軟體，利用搜尋引擎最佳化／購買關鍵字廣告(SEO)來大肆散播

Cisco Talos 資安研究人員發現 DragonRank 威脅組織發動全新惡意攻擊行動。據報導，攻擊者利用搜尋引擎最佳化／購買關鍵字廣告 (SEO) 伎倆來部署惡意 webshell、從受感染系統收集資訊以及傳送 PlugX 和 BadIIS 惡意軟體有效酬荷。該威脅組織還在攻擊中利用各種工具進行憑證轉存，包括 Mimikatz、PrintNotifyPotato 或 BadPotato。此攻擊行動鎖定亞洲和歐洲的各行各業。

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-RLsass!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30
- SONAR.TCP!gen1
- 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：

- DDoS.Trojan
- Hacktool.Mimikatz
- Infostealer
- Meterpreter
- Trojan Horse
- Trojan.Badiis!g1
- Trojan.Certbypass
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Malscript
- 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

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。

2024/09/12

全球勒索軟體活動在2024年第二季出現激增

勒索軟體活動在 2024 年第二季顯著增加，因為攻擊者似乎在 2023 年底和 2024 年初的執法單位進行執法行動後又捲土重來，並且更加興致勃勃。從 Ransomware Leak Sites 資料分析發現，勒索軟體攻擊者在 2024 年第二季聲稱發動 1,310 次攻擊，較今年第一季增加 36%。這是勒索軟體業者在一個季度內宣稱的第二高攻擊數量，少於 2023 年第三季度宣稱的 1,488 次攻擊記錄。

請參閱我們的部落格：全球勒索軟體活動再度逼近歷史高峰。

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：

- Ransom.Akira
- Ransom.Basta
- Ransom.Bianlian
- Ransom.Blacksuit
- Ransom.Cactus
- Ransom.Cl0p
- Ransom.Hunters
- Ransom.Lockbit
- Ransom.PlayCrypt
- Ransom.Phobos
- Ransom.Qilin
- Ransom.Ransomhub

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: MOVEit Transfer RCE CVE-2023-34362
- Web Attack: CrushFTP CVE-2024-4040

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.B
- Heur.AdvML.C

2024/09/12

SuperShell惡意軟體的後繼最新版本，鎖定Linux SSH伺服器威攻擊目標

SuperShell 惡意軟體的後繼最新版本在最近的攻擊行動中被發現到，目標是易受攻擊或配置錯誤的 Linux SSH 伺服器。此惡意軟體以 Go 為基礎，具有作為反向 shell 的功能，可有效允許攻擊者在受感染的機器上進行遠端控制和遠端程式碼執行。遭 SuperShell 惡意軟體入侵的伺服器很可能會被攻擊者用來進行挖礦或發動 DDoS 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：

- Downloader
- PUA.Gen.2
- Trojan.Gen.NPE

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。

2024/09/11

ScRansom勒索軟體

研究人員發現 CosmicBeetle 威脅組織正在濫用全新 ScRansom 勒索軟體，取代他們舊有的 Scarab 勒索軟體。他們目標是全球的中小型企業，並在勒索贖金支付通知和網站的風格上模仿 LockBit。CosmicBeetle 威脅組織被懷疑與 RansomHub 有關聯，RansomHub 是最近活躍的勒索軟體團體，自 2024 年 3 月以來不斷增加其行動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Spacecolon
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C

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。

2024/09/11

中國進階持續威脅駭客組織(APT)濫用VSCode

Stately Taurus 是一個執行網路間諜攻擊的中國進階持續威脅駭客組織 (APT)，已經在針對東南亞政府單位的間諜行動中濫用 Visual Studio Code 軟體。此威脅組織濫用 VSCode 的內嵌反向 shell 功能，在目標網路中取得立足點，以執行任意程式碼並傳送額外的有效酬載。威脅者利用此機制來傳送惡意軟體、執行偵查及外洩敏感資料。

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

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.Shadowpad
- Infostealer
- Ransom.Zombie
- 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!400
- Heur.AdvML.A!500
- 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。

2024/09/11

在真實網路情境上發現Cicada3301勒索軟體的最新變種

根據 Palo Alto 最近一份報告，Repellent Scorpius 是一個新曝光的勒索軟體即服務 (RaaS) 駭客組織，負責傳送被稱為 Cicada3301 的勒索軟體最新變種。據觀察，威脅份子在攻擊中利用多種就地取材 (Living-Off-the-Land：LOTL) 工具。其中 PsExec 用於執行勒索軟體，而 Rclone 工具則用於資料外洩。Cicada3301 是基於 Rust 的勒索軟體，使用 ChaCha20 加密演算法來加密使用者檔案。此惡意軟體最新變種包含一些新增功能，例如：新的令列參數或新的 PowerShell 指令，允許其停止在受感染系統上執行的虛擬機器。

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：

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

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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。

2024/09/11

Mekotio和BBTok這兩種銀行木馬，仍然在拉丁美洲和加勒比海地區大肆氾濫

Mekotio 和 BBTok 惡意軟體仍然是最近在拉丁美洲地區散佈的銀行特洛伊木馬家族中活躍分子。惡意軟體通常透過以商業或司法為主題的釣魚行動進行散佈。垃圾郵件會利用連結誘導惡意檔案下載，或直接在垃圾郵件中使用惡意附件。Mekotio 是較舊的惡意軟體，而 BBTok 則是在 2020 年才被發現。這兩個惡意軟體都以類似區域為目標，並試圖滲出憑證和敏感資訊，以執行未經授權的銀行業務。

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：

- ISB.Downloader!gen294
- Trojan Horse
- Trojan.Gen.MBT
- 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：

- 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。

2024/09/11

威脅者偽造愛爾蘭郵政服務以竊取憑證

賽門鐵克發現新一波的網路釣魚攻擊，這些攻擊假冒愛爾蘭國有郵政服務供應商 (An Post Ireland) 來竊取憑證。在這一波攻擊中，釣魚電子郵件偽裝成包裹通知，以重新安排遞送時間或檢查包裹詳細資料。電子郵件內容簡短，鼓勵收件者點選網路釣魚網址。一旦點選，受害者就會遇到專為收集憑證而設計的網頁。

- 電子郵件主旨：We were trying to deliver your parcel *我們正嘗試遞送您的包裹
- 電子郵件來自 An Post Ireland <假冒的郵件位址>

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)。

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。

2024/09/11

透過影像掃描竊取加密貨幣錢包的手機／行動惡意軟體：SpyAgent

一款名為 SpyAgent 新型手機／行動惡意軟體，透過掃描您裝置上可能包含助記詞的圖片來作目標式攻擊。助記詞是用於復原加密貨幣錢包 12 個單字的英文單詞。這些密語對威脅份子而言非常有價值，因為取得這些密語後，他們就能在自己裝置上還原您的錢包，並竊取錢包內儲存的所有資金。

SpyAgent 會將自己偽裝成各種可信賴的 APP，包括銀行、政府服務、串流平台和公用程式等 APP。安裝後，這些偽造 APP 會秘密收集您的文字訊息、聯絡人和儲存的影像，並傳送至遠端伺服器進行 OCR 掃描。為了避免被偵測到，SpyAgent 可能會使用一些策略，例如：無止盡的載入畫面、非預期的重導向或短暫的空白畫面。此外，SpyAgent 可從其命令與控制 (C&C) 伺服器接收指令，以更改聲音設定或傳送簡訊，並可能散佈釣魚簡訊，進一步散播惡意軟體。

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：

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.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。

2024/09/11

Loki Backdoor後門程式出現新變種：採用Mythic Framework和Havoc技術

新版本 Loki 後門被發現以俄羅斯組織為目標。此變種與 Mythic 框架相容，並利用 Havoc 框架的各種技術，使分析變得複雜。更新後的變種分為惡意程式載入器及 DLL。惡意程式載入器從被入侵的機器收集系統資訊，上傳至攻擊者的 C&C 伺服器，並擷取 DLL 作為回應。然後將 DLL 載入記憶體，下載額外的有效酬載，並推進下一步的攻擊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Sc!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.Cobalt
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- 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
- 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。

2024/09/10
防護亮點：賽門鐵克端點上的網路層入侵防護系統(IPS)的稽核特徵，精準發現兩用工具的異常活動

兩用工具

所謂兩用工具，即本身是可運行在電腦中的合法工具，但可被惡意威脅者用來發動攻擊。此類攻擊讓攻擊者不需另外撰寫惡意程式，因其工具的合法特性不易被使用者或安全工具偵測，也更難被追蹤和特定組織的關聯性。常見的兩用工具會隨作業系統一起安裝或常見的網管或遠端連線軟體。例如：Psexec、Nmap、Remote Desktop、AnyDesk。對於許多最近的威脅 (例如：RansomHub)，兩用工具被觀察到是攻擊鏈的一部分。網路掃描工具和遠端存取軟體被攻擊者用來探索受害者網路樣貌和橫向移動。在部署勒索軟體之前，通常會看到這些工具的活動。

賽門鐵克的端點上網路層入侵防護系統(IPS)之稽核特徵

賽門鐵克端點上的網路層入侵防護系統 (IPS) 引擎的主要功能之一是稽核特徵。這些稽核特徵有許多是常用於針對勒索攻擊等的雙重用途工具，已知 RansomHub 所屬的組織會利用這些工具進行橫向移動。對於不使用這些工具執行日常裝置管理任務的管理員而言，稽核特徵有助於通知網路內的不尋常活動。

政策組態

SEP 管理員可以設定政策，將稽核特徵動作設定為允許或封鎖，並將特徵記錄設定為記錄或不記錄。預設情況下，這些稽核特徵會設定為允許和不記錄流量。Broadcom 的線上技術文件說明可引導如何設定 SEP 並變更 IPS 稽核特徵偵測的動作。

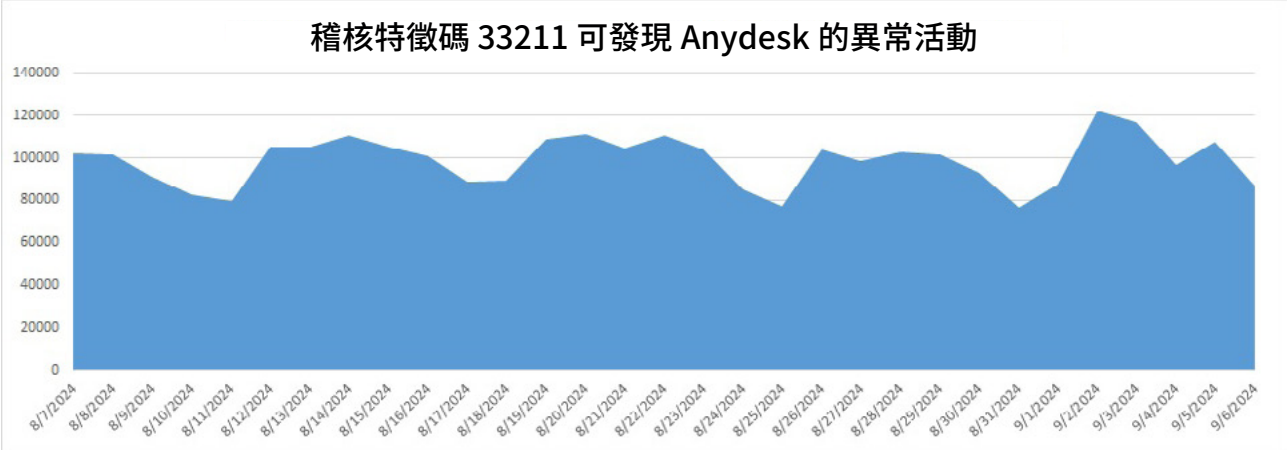
RansomHub與兩用工具防護

以下是賽門鐵克發佈一些 IPS 稽核特徵，用於偵測兩用工具。根據定義，並非所有使用這些工具的行為都是惡意，但特徵名稱中提及的程式已知會在 RansomHub 感染前的階段出現。

- 30068 - Audit: PSExec Utility Activity
- 34633 - Audit: FileZilla SFTP Activity
- 33290 - Audit: Network Scanner Activity
- 33588 - Audit: WMIC Remote RPC Interface Bind Attempt
- 33211 - Audit: AnyDesk Remote Desktop Activity
- 34540 - Audit: Anydesk Tool Download
- 34697 - Audit: WinSCP Connecting to Public IP
- 33119 - Audit: RClone Tool Activity
- 33256 - Audit: RClone Tool Activity 2
- 34781 - Audit: RClone MegaSync Connect
- 34796 - Audit: RClone Tool Activity 3

稽核特徵碼33211--AnyDesk Activity

以 ID 33211--Audit：AnyDesk Remote Desktop Activity為例。賽門鐵克 IPS 每天都會在所有 SEP 端點上出現此特徵碼平均攔截約 100,000 次網路流量嘗試，因為 SEP 客戶已採取行動設定入侵防護政策，選擇加入此攔截動作。



*** SEP 的稽核特徵碼主要在提高對網路中可能不需要流量的警覺性。預設情況下，它們不會封鎖。管理員檢閱其網路上 IPS 事件日誌時，可以注意到這些稽核事件，並決定是否設定相對應的稽核特徵碼以封鎖流量。*

建議客戶在桌機／筆電和伺服器上啟用 IPS，以獲得最佳保護。請點擊此處瞭解啟用 IPS 的說明。
欲瞭解如何整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站，請點擊此處。
沒有使用 SEP 也行？可使用賽門鐵克瀏覽器防護服務保護您的瀏覽器。
欲瞭解賽門鐵克的端點上的網路層入侵防護系統 (IPS) 的稽核特徵，請點擊此處。

2024/09/10

假冒防毒軟體部署遠端有效酬載的惡意軟體Latrodectus散播行動

據報導，有一個偽裝成合法防毒軟體廠商 Latrodectus 惡意軟體攻擊行動出現。最初攻擊媒介包括網路釣魚和惡意廣告。Latrodectus 具備後門功能，允許執行遠端指令和部署 Brute Ratel C4 等惡意有效酬載。它採用常見的常駐技術，包括使用 Windows Component Object Model (COM)，並採用 TLS 憑證與其命令與控制 (C&C) 伺服器進行通訊。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen609

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
- Web.Reputation.1
- 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。

2024/09/10

CVE-2024-45195：存在Apache OFBiz中的遠端執行程式碼(RCE)漏洞

CVE-2024-45195 是 Apache OFBiz (一套全面的商業應用程式) 中的高嚴重性 (CVSS 風險評分：7.5) 遠端執行程式碼 (RCE) 漏洞。攻擊者可透過繞過認證通訊協定的特殊設計網頁來開採濫用該漏洞。如果被成功開採濫用，此漏洞將允許遠端攻擊者在伺服器上執行惡意程式碼，可能導致系統完全受損。此漏洞會影響 Apache OFBiz：18.12.16 之前的版本。賽門鐵克的入侵防護系統 (IPS) 可針對這些入侵嘗試提供防護，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-2024-45195
- Web Attack: Apache OFBiz RCE Vulnerability CVE-2024-38856

2024/09/10

地理位置資訊伺服器GeoServer重大層級已知漏洞：CVE-2024-36401，已被持續開採濫用出現實際攻擊行動

多起攻擊行動正在開採濫用 OSGeo GeoServer GeoTools 最近被揭露的安全漏洞。該漏洞被識別為 CVE-2024-36401(CVSS 風險評分為 9.8)，是一個重要的遠端程式碼執行漏洞 (RCE)，允許惡意使用者控制受影響的機器。此漏洞已被開採濫用來部署 GOREVERSE，這是一個反向代理伺服器，設計用來與命令與控制 (C&C) 伺服器連線，以進行攻擊後的活動。遭入侵的伺服器已被用來傳送加密貨幣挖礦程式、Condi 和 JenX 等殭屍網路惡意軟體，以及一個名為 SideWalk 的知名進階 Linux 後門。

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：

- CL.Downloader!gen277
- Linux.Mirai
- Linux.Mirai!g2
- Trojan.Gen.NPE
- Trojan.Gen.NPE.2
- Trojan Horse
- WS.Malware.1
- WS.SecurityRisk.4

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。

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: GeoServer RCE Vulnerability CVE-2024-36401
- Web Attack: GeoServer RCE Vulnerability CVE-2024-36401 2
- Web Attack: GeoServer RCE Vulnerability CVE-2024-36401 3

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 UNIX 強化保護政策可設定成停用反向連線、允許已建立的相關連線，並只允許 DNS、HTTP 和 HTTPS 等必要的出埠流量。客戶也應停用 WFS 請求，直到將 GeoServer 升級至已修補的版本。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2024/09/09

TIDRONE駭客組織，發動對台灣的攻擊活動

最近有消息指出，TIDRONE 駭客組織針對台灣的軍事與衛星產業，將無人機製造商列為攻擊目標。該組織利用 CXCLNT 和 CLNTEND 等惡意工具，實現資料竊取、憑證傾印和使用者控制繞過。根據報導，他們的策略、技術與程序 (TTPs) 包括透過 ERP 軟體進行供應鏈攻擊，應屬間諜動機。

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 Horse

基於機器學習的防禦技術：

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

2024/09/08

源於開放原始碼的Babylon遠端存取木馬(RAT)：鎖定馬來西亞發動攻擊

源於開放原始碼的 Babylon 遠端存取木馬 (RAT)，最近針對馬來西亞大肆氾濫。攻擊鏈包含使用精心製作的 .iso 檔案假冒成 PDF 文件檔。傳送 ISO 檔包含一個隱藏的 PowerShell 指令碼、一個偽裝的 PDF 文件檔和一個惡意的可執行檔，最終會導致感染 Babylon RAT。此遠端存取木馬允許攻擊者進行廣泛的間諜和資訊竊取活動，包括竊取憑證和剪貼簿內容、鍵盤記錄以及遠端命令執行。

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.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：

- Scr.Mallnk!gen12
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Reputation.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。

2024/09/08

ToneShell後門鎖定英國智庫國際戰略研究所(International Institute for Strategic Studies，IISS)的高峰論壇為目標

據報導，Mustang Panda 駭客組織發起一場 ToneShell 惡意後門程式涉入的網路間諜行動，目標是 2024 年11月8～10日在布拉格 IISS 國防高峰會的與會者。該攻擊利用偽裝成高峰會文件的惡意 PIF 檔，以取得敏感國防議題的存取權。惡意軟體透過機碼裡的 run 值和排程工作達到持續性，並使用假冒原始 TCP 的 TLS 原始 TCP 與香港 C&C 伺服器通訊。

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：

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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2024/09/06

Quasar遠端存取木馬(RAT)的後繼新變種涉入由BlindEagle威脅組織針對哥倫比亞保險業所發動的網路攻擊

BlindEagle 是一個進階持續性威脅組織 (APT)，已被發現到濫用 BlotchyQuasar 遠端存取木馬程式 (RAT) 來攻擊哥倫比亞的保險業。攻擊鏈由冒充哥倫比亞稅務機關的釣魚電子郵件開始，其中包括存放在遭入侵的 Google Drive 帳戶上的惡意軟體連結。BlotchyQuasar 是 QuasarRAT 的重度混淆變種，可進行鍵盤側錄、憑證竊取和銀行活動監控。它透過動態 DNS 服務和 VPN 與指揮和控制 (C&C) 伺服器通訊，突顯其精密的迴避策略。

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
- ACM.Untrst-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g250

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!gdn33
- Scr.Malcode!gdn34
- Trojan.Gen.MBT

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。

2024/09/06

Tropic Trooper威脅組織發表全新的China Chopper惡意程式及Crowdoor惡意程式載入器

據報導，會講中文的 Tropic Trooper 威脅組織已經鎖定中東國家的政府單位來發動間諜行動。攻擊者專注於與人權研究相關的系統，使用部署在被入侵的 Umbraco CMS 伺服器上全新 China Chopper 惡意程式。該威脅組織使用 DLL 劫持來載入惡意有效酬載，包括與 SparrowDoor 後門連結的惡意程式載入器：Crowdoor。

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
- WS.Reputation.1
- 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

- 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。

2024/09/06

垃圾郵件發送者濫用罕見的頂級域名(TLD)

賽門鐵克最近發現到一起全新的網路釣魚行動，該行動是透過最近建立的網域來竊取認證和／或銀行資訊。在這次行動中，我們發現到超過 200 個新註冊的網域，這些網域大多以罕見的頂級域名 (TLD) 註冊，例如：「.best」、「.rest」或「.shop」。這些郵件的主旨和內文試圖透過誇大效用的健康產品來引誘收件者。

主旨範例：

- Sleep Your Way to Fat Loss: Try This Rice Trick Tonight! 睡覺就能減脂：今晚就試試這個神奇的米飯！
- THIS everyday food is making your vision WORSE ¦ 遠離傷害你的視力的這些日常食物
- bone on bone...*骨頭相互摩擦的疼痛和如何保護你的膝蓋
- 119 men have just said goodbye to ED forever! *119 位男性剛擺脫勃起功能障礙的困擾！
- Those who ate THIS common food had WORSE vision loss *吃這種常見食物的人，視力衰退每況愈下。

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)。

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。

2024/09/06

假冒跨國石化合資企業的詢價單，發動全球性的Formbook惡意竊密程式攻擊行動

賽門鐵克最近觀察到一起 Formbook 惡意竊密程式攻擊行動。攻擊者冒充一家位於德國的全球化工公司和馬來西亞的國家石油與天然氣公司之間的主要合資企業。在這個惡意電子郵件攻擊行動中，他們的目標是多個國家和不同行業領域的公司，包括：

- IT 與諮詢
- 製藥與醫療保健

- 物流與供應鏈
- 金融服務
- 工程與工業解決方案
- 生物科技與生命科學
- 媒體與出版
- 電信與科技
- 橡膠與工業製造
- 運動器材
- 化學品與材料
- 葡萄酒和飲料分銷
- 海運與航運
- 家具製造
- 能源與電力
- 汽車與精密製造

該封電子郵件 (主旨：[偽造的公司名稱] Request For Quotation) 被設計成來自合資企業採購經理的正式邀請，邀請收件人的公司參加即將進行旋轉設備服務相關的供應商招標資格預審活動。該電子郵件列出收件人公司必須提交的幾份文件，包括 KYC 問卷、行為守則、聲明書和各種資格預審表格。

最後截止期限為 2024 年 9 月 13 日，若未回應則被認為對投標沒有意願。此用意在迫使使用者執行 Formbook 的二進位檔案，該檔案偽裝成 RFQ([偽造的公司名稱]Request For Quotation.exe)，包含在附加的檔案 ([偽造公司名稱] Request For Quotation.zip) 中。

Formbook 是一種在駭客圈備受推崇且非常盛行的惡意竊密程式，多年來一直是威脅生態圈的要角，全球各地的各種駭客組織與個體戶都在使用。

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：

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)。

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
- Trojan Horse

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：

- System Infected: Trojan.Formbook Activity 2
- Web Attack: Webpulse Bad Reputation Domain Request

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求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。