保安資訊--本周(台灣時間2024/08/16)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 9,300 台受保護端點上總共阻止了 4,740 萬次攻擊。這些攻擊中有 82.5% 在感染階段前就被有效阻止：**(2024/08/12)**

- 在**8萬7,400**台端點上，阻止了**1,170**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**11萬4,100**台端點上，阻止了**940**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬2,000**台**Windows**伺服主機上，阻止了**74**萬次攻擊。
- 在**5萬4,700**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,200**台端點上，阻止了**66萬4,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬600**台端點上，阻止了**260**萬次嘗試利用的應用程式漏洞。
- 在**14萬7,700**台端點上，阻止了**530**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,000**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬2,300**台端點上，阻止了**720**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**653**台端點上，阻止了**8萬5,800**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 200 個受保護端點上阻止了總計 330 萬次攻擊。**(2024/08/12)**

- 使用網頁信譽情資，在 **101.7K** 個端點上阻止 **280** 萬次攻擊。
- 攔截 **18.9K** 個端點上 **366.5K** 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 **6.3K** 個端點上攔截 **66.7K** 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 **194** 個端點上攔截 **6K** 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。

2024/08/15

由Go程式撰寫的Cyclops惡意軟體

Cyclops 是最近發現的一個 Go 語言惡意軟體植入程式，很可能是 BellaCiao 惡意軟體系列的繼任者。已知的惡意軟體二進位檔偽裝成「Microsoft SqlServer.exe」可執行檔，試圖冒充 SQL 伺服器更新檔案，並可能部署在其他易受攻擊的伺服器機器上。Cyclops 允許攻擊者從受感染的機器中滲出檔案，並在受感染的機器上執行任意檔案。一旦部署，Cyclops 會透過 SSH 通道啟動 HTTP 服務，允許操作者在目標系統上啟動指令。

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：

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

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。

2024/08/15

Pupy遠端存取木馬(RAT)涉入最近由UTG-Q-010 APT駭客組織發動地網路攻擊行動

據報導，Pupy 遠端存取木馬 (RAT) 在歸屬於 UTG-Q-010 威脅組織的新行動中被散佈。攻擊者利用包含加密貨幣誘惑的網路釣魚郵件或偽裝成求職履歷的電子郵件。攻擊鏈涉及使用內嵌 DLL 載入器的惡意 .lnk 檔案，最後在 Pupy RAT 有效酬載部署。Pupy 是一種基於 Python 的遠端存取木馬程式 (RAT)，具有反射式 DLL 載入和記憶體內執行等功能。

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：

基於行為偵測技術(SONAR)的防護：

- 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：

- Scr.Heuristic!gen20
- Scr.Mallnk!gen10
- Scr.Mallnk!gen12
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2024/08/15

發現針對Windows和Linux系統發動攻擊的工具和批次腳本越來越多

根據 DFIR(Digital Forensics and Incident Response)：數位鑑識與資安事件分析及處理，最近一份報告，已發現一系列的威脅者工具，可以繞過 Windows Defender 和 Malwarebytes 等安全防護系統、刪除備份和停用系統。在已發現的工具中，包括用於代理服務和 SystemBC 的 Ngrok，以及兩個知名的命令與控制框架：Sliver 和 PoshC2。最近活動是在 2024 年 8 月偵測到。

報告中還詳細說明發現一個包含各種批次腳本的開放目錄。分析顯示，這些腳本以 Windows 和 Linux 系統為目標，在攻擊的各個階段中都會被利用。它們在攻擊鏈的每個階段中扮演重要角色，執行的任務包括停用安全措施、停止主要服務，以及建立命令與控制通道。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Net!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Schtsk!g1
- ACM.Ps-Sc!g1
- ACM.Ps-Wbadmin!g1
- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen14
- SONAR.SuspLaunch!g193

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
- Downloader
- PoshC2!gen4
- Scr.Malscript!gen1
- Scr.Malcode!gen74
- Trojan Horse
- 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
- Heur.AdvML.B!100
- Heur.AdvML.B!200eur.AdvML.A

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: Atera Client Activity

2024/08/14

要被遠端連線前，請再三確認～以好工具AnyDesk和Microsoft Teams來做壞事的惡意郵件攻擊行動

研究人員最近發現另一種更大膽的電子郵件釣魚、殺魚行動，初始是釣魚郵件、之後透過 Microsoft Teams 進行語音通話。攻擊者說服受害者下載遠端存取工具 AnyDesk，讓他們控制受害者的電腦。一旦取得控制權，攻擊者就會執行惡意有效酬載，並從系統中竊取資料。

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：

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
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

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

2024/08/14

全新的macOS惡意竊密程式使用SwiftUI和OpenDirectory API竊取憑證

最近有報導一款全新的多階段 macOS 惡意竊取程式。此惡意軟體呈現以下許多特徵：

- 採用 SwiftUI 來提示密碼
- 使用 OpenDirectory API 來驗證擷取的密碼
- 使用各種 API 來逃避偵測

一開始它會執行一個以 Swift 撰寫的誘捕程式，顯示假的密碼提示來欺騙使用者。擷取憑證後，惡意軟體會使用 OpenDirectory API 驗證憑證，再從命令控制伺服器下載並執行惡意指令碼。

網路知識：2019 年的 WWDC 中，Apple 宣布一個名為「SwiftUI」的全新框架，這讓所有的開發者都大為驚訝，它不僅改變開發 iOS App 的方式，也是自 Swift 問世以來 Apple 開發者的生態系統 (包括 iPadOS、macOS、tvOS 與 watchOS) 的最大轉變。SwiftUI 是一種創新且極為簡單

的方式，透過 Swift 強大功能，可在所有的 Apple 平台上建立使用者介面。只需使用一套工具與 API，即可為所有的 Apple 裝置建立使用者介面。

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

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。

2024/08/14

.shop通用頂級網域名稱成為傳播加密貨幣垃圾郵件浪潮的新寵兒

最近，.shop 的通用頂級網域名稱被威脅者大量濫用傳播加密貨幣垃圾郵件。.shop 的通用頂級網域名稱於 2016 年推出，專為線上購物或電子商務平台設計，零售商和電子商務商店等均可使用。賽門鐵克已觀察到持續不斷的垃圾郵件浪潮，誘使電子郵件使用者點選短網址，進而重導向至託管加密貨幣相關內容的假 .shop 通用頂級網域。

這些以加密貨幣為主題的垃圾郵件有以下特徵：

- 電子郵件主題是隨機的名字和姓氏，並透過濫用免費電子郵件用戶服務發送。
- 電子郵件的本文部分沒有或只有很少的內容。
- 偽造或可疑的 .shop gTLD 加密貨幣網域會在電子郵件本文部分且隱藏在縮短的 URL 中。
- 與這些運作相關的網域註冊期限為 1 或 2 年。
- 一旦點擊，電子郵件使用者就會看到假的或偽造的加密貨幣促銷網頁。

在這些運行中使用縮短的 URL 顯示可能會增加點擊率，因為它們看起來是合法的，很可能會被點擊。

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：

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。

2024/08/14
Datablack勒索軟體

Datablack 是在真實網路情境上觀察到的全新勒索軟體。該勒索軟體與知名 Proton 惡意軟體家族的勒索軟體類型有相似之處。Datablack 會加密使用者檔案，並在重新命名的檔案名稱中冠上 .Datablack 副檔名。勒索軟體支付說明是以一個名為 #Recovery.txt 的文字檔形式儲存，攻擊者要求受害者透過提供的電子郵件帳號與他們聯絡，以取得有關資料解密的進一步指示。該惡意軟體具有從受感染的機器中移除磁碟陰影複本以及在啟動過程中停用自動修復選項的功能。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g340

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

2024/08/14
全新Gigabud手機／行動惡意程式可能與Golddigger木馬程式有所關聯

在真實網路情境中發現安卓平台上 Gigabud 惡意軟體的新變種。雖然這種惡意軟體初始變種至少在 2023 年就已為人所知，但最新變種的散佈範圍已擴大，現在目標是全球各個國家。惡意軟體通常會透過偽裝成 Google Play 商店的釣魚網站或冒充各種銀行或政府單位的網站散佈。該惡意軟體具有多種功能，例如：收集受感染裝置資料、洩露銀行憑證、收集螢幕錄影等。最新 Gigabud 變種在程式碼和採用技術上與另一個被稱為 Golddigger 手機惡意軟體家族有某些相似之處。

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
- 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。

2024/08/14

CVE-2024-38856--存在Apache OFBiz允許未經身份驗證的遠端程式碼執行漏洞

CVE-2024-38856 是最近被揭露的嚴重等級 (CVSS 風險評分：9.8) 允許未經身份驗證的遠端程式碼執行漏洞，會影響 Apache OFBiz 18.12.14 之前的版本。此漏洞源自於覆蓋視圖功能的漏洞。一旦被利用，未經驗證的攻擊者可透過精心製作的請求遠端執行程式碼。應用程式供應商已釋出修補程式，在 18.12.15 或更新版本的產品中解決這個漏洞。

網路知識：Apache OFBiz 專案是一項開放源碼的企業自動化軟體專案。許多軟體開發商會利用這個專案來開自己的開源企業資源規劃 (ERP)、開源客戶關係管理 (CRM)、開源電子商業／電子商務 (E-Business/E-Commerce)、開源供應練管理 (SCM)、開源生產資源規劃 (MRP)、開源電腦化維修管理系統／企業資產管理 (CMMS/EAM)……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：

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 RCE Vulnerability CVE-2024-38856

2024/08/14

Allarich勒索軟體

最近勒索軟體生態圈出現一款名為 Allarich 的全新型勒索軟體。它會加密檔案，並冠上「.allarich」副檔名，還會變更桌面桌布。在完成加密程序後，勒索軟體會產生一個檔名為「README.txt」的勒索贖金支付說明文字檔。

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.Cryptlocker!g38

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.Allarich
- 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

2024/08/13
防護亮點：賽門鐵克EDR如何有效防護--Impacket遭濫用且扶搖直上的危害

Impacket 網路滲透測試工具

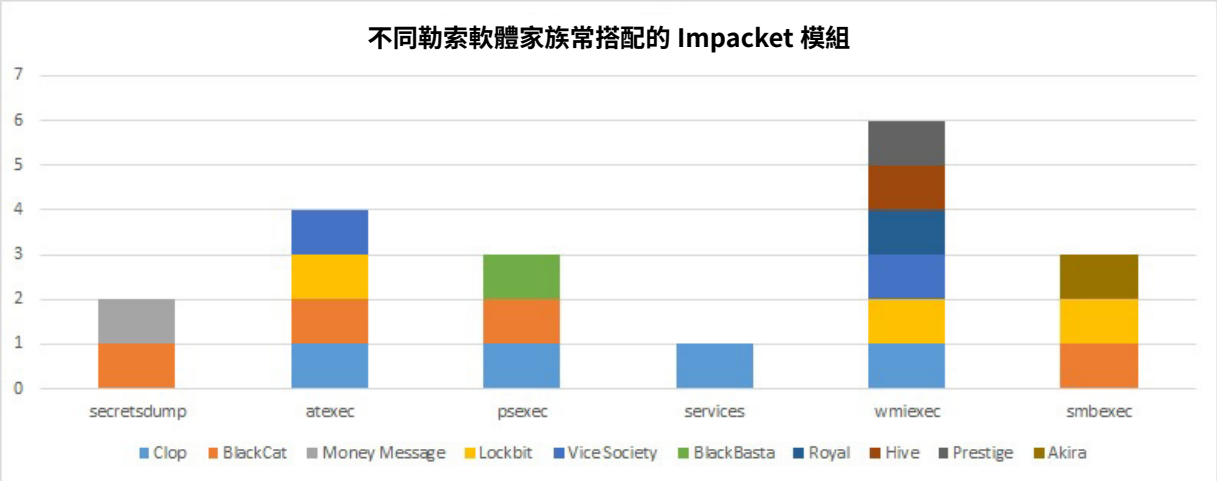
近來有多種工具可用於網路滲透測試。Impacket 是炙手可熱且功能強大的工具套件組合 (包)，已在駭客圈獲得極高知名度，它是採用 Python 撰寫，可說是專為操控網路封包所寫的開放原始碼大集合，可讓開發人員製作和解碼網路封包。它支援 IP、UDP、TCP、SMB、MSRPC 及其他數種網路通訊協定。Impacket 深受合法滲透測試者的歡迎，但也逐漸受到網路罪犯的青睞。

Impacket 的主要特色

- 支援最多樣的通訊協定
- 易於操控通訊協定
- 操控 SMB 檔案存取儲存協定和 NTLM 安全協議
- 操控微軟遠端程序呼叫 (MSRPC) 通訊協定
- 密碼攻擊與破解

一個令人不安的趨勢是，威脅份子似乎越來越依賴 Impacket 來進行橫向移動和遠端執行，特別是觀察到勒索軟體威脅分子濫用 Impacket。

以下是勒索軟體最常使用的模組及其使用方法。



Impacket 用於遠端執行的常見模組

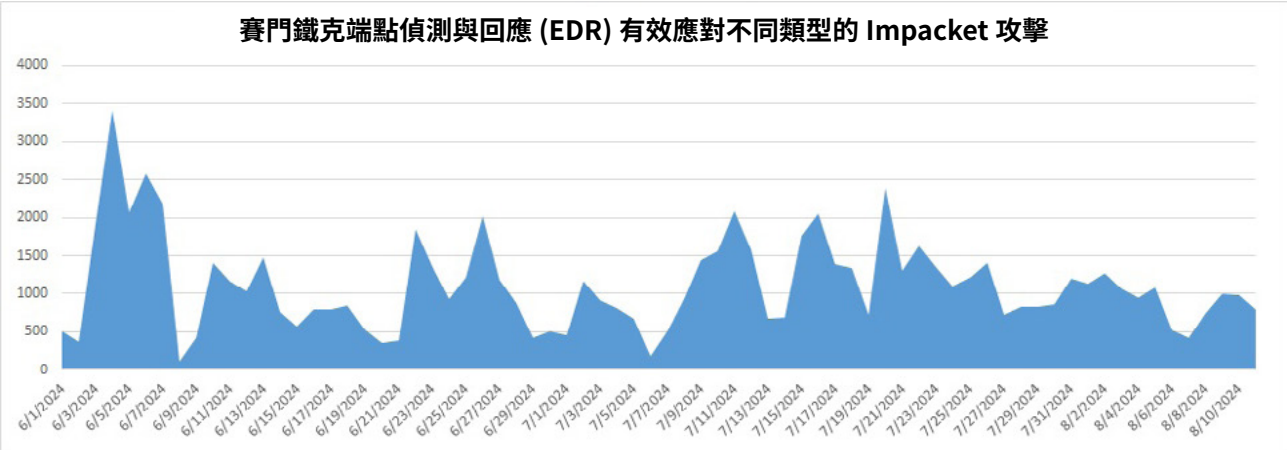
- **atexec**：此模組被用於工作排程服務在遠端機器上執行指令
  - 命令列：
    - cmd.exe /C systeminfo > CSIDL_WINDOWS\temp\<random>.tmp 2>&1
    - cmd.exe /C powershell -ep bypass -f CSIDL_WINDOWS\temp\<random>.ps1 > CSIDL_WINDOWS\temp\<random>.tmp 2>&1
- **psexec**：這個模組提供 psexec 功能在遠端機器上執行有效酬載
  - 方法：
    - 在遠端機器上寫 beakon 到 ADMIN$ 路徑
    - 建立隨機服務："HKLM\SYSTEM\CurrentControlSet\Services\<random_name>"
- **services**：此模組在遠端機器上建立服務
  - 方法：
    - services.exe 建立服務機碼 "HKLM/SYSTEM/CurrentControlSet/Services/<random_name>"
- **wmiexec**：這個模組提供 WMI 功能來提供反向 shell
  - 命令列：
    - CSIDL_SYSTEM\wbem\wmic.exe /node:%cn% process call create CSIDL_SYSTEM_DRIVE\temp\<random>.bat
- **smbexec**：這個模組提供反向 shell
  - 命令列
    - CSIDL_SYSTEM\cmd.exe /Q /c echo cd ^> \<6,47856BB5>\C$__output 2^>^&1 > CSIDL_WINDOWS\<random>.bat & del CSIDL_WINDOWS\<random>.bat

Impacket 用於憑證盜用的常見模組

- **secretsdump**：此模組用於轉存遠端機器的憑證
  - 命令列：
    - CSIDL_SYSTEM\svchost.exe -k localService -p -s RemoteRegistry
    - esentutl.exe /y "CSIDL_PROFILE\dragos\appdata\local\google\chrome\user data\default\login data" /d "CSIDL_PROFILE\dragos\appdata\local\google\chrome\user data\default\login data.tmp"。

EDR(端點偵測與回應)事件建立

賽門鐵克端點偵測與回應 (EDR：Symantec Endpoint Detection and Response) 使用機器學習和行為分析來偵測和揭露可疑的網路活動。EDR 會針對潛在的有害活動發出警示，排定事件的優先順序以進行快速分流 (類似災難現場的檢傷分類)，並允許事件回應人員瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。



威脅獵捕查詢

賽門鐵克 EDR 客戶可在以下連結找到威脅獵捕查詢。

- https://github.com/Symantec/threathunters/tree/main/ImPacket

欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

2024/08/13

假冒Google安全中心的網路釣魚行動

據報導，一個冒充 Google 安全中心的網路釣魚行動正在誘騙使用者下載一個偽裝成第二個步驟驗證身分驗證 APP：Google Authenticator 的惡意檔案。這個檔案會安裝兩種惡意軟體：Latrodectus 是一個下載程式，會執行 C&C 伺服器的指令，而 ACR Stealer 則會使用 Dead Drop Resolver 來隱藏其 C&C 伺服器的詳細資訊。該行動展示進階的迴避技術，並持續努力改進惡意軟體的功力。

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.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- 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：

- Audit: Bad Reputation Application Activity

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。

2024/08/13

ABCloader惡意程式涉入Actor240524駭客集團對亞塞拜然和以色列發動的目標式網路釣魚行動

新冒出頭的Actor240524 駭客集團，針對亞塞拜然和以色列進行魚叉式網路釣魚行動。使用者會被偽裝的政府官方文件誘騙，這些文件包含內嵌的 VBA 巨集，執行時會傳送 ABCloader 惡意程式的有效酬載。ABCloader 會解密並載入 ABCsync DLL，然後與 C&C 伺服器通訊以取得遠端指令。惡意軟體採用反沙箱和反偵錯技術來逃避偵測。

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：

自適應防護技術(包含於SESC)：

- ACM.Word-CPE!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!gen433
- W32.Silly!gen
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- WS.Malware.1

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

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。

2024/08/13

網路釣魚攻擊透過Discord的內容派送網路(CDN)來儲存及散播0bj3ctivity惡意竊密程式

據報導，由 Ande Loader 惡意軟體觸發初始攻擊的網路釣魚行動最終會散播 0bj3ctivity 惡意竊密程式。此攻擊借力於 Discord 的內容派送網路 (CDN) 架構，其中包含內嵌 PowerShell 指令碼的惡意 JavaScript 檔案，以部署其他的有效酬載。Ande Loader 用於初始感染和持續感染。惡意竊密程式會將敏感資料從瀏覽器滲出到 Telegram 或 C&C 伺服器，並包含反偵錯和反虛擬環境 (anti-VM) 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.AdInPr-Lnch!g1
- ACM.Ps-Base64!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-RgPst!g1
- ACM.Wscr-Ps!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g20
- SONAR.PsEmpire!gen8

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!gen11

- Downloader
- ISB.Downloader!gen40
- ISB.Heuristic!gen58
- Scr.Malcode!gdn14
- Trojan.Malimg
- 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

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。

2024/08/12

Grayfly駭客集團不斷引進全新的惡意程式載入程式和不同手法創造天時地利的攻擊條件

Grayfly 駭客集團 (也稱為 Earth Baku) 已被觀察到從印太地區擴大到全球範圍，目標為醫療保健、媒體、政府、教育等領域。在最近一場攻擊行動中，威脅份子利用 IIS 伺服器等提供網際網路服務的應用程式進行初始存取，並部署 Godzilla webshell 進行控制。該駭客集團已引入全新的惡意程式載入程式，包括 StealthVector 和 StealthReacher，以隱匿方式啟動後門元件，並新增 SneakCross 作為其最新的模組化後門。

在攻擊鏈的後期階段，Grayfly 使用多種工具，包括自訂的 iox 工具、Rakshasa 和 Tailscale 來進行常駐，以及 MEGAcmd 來將資料有效地滲出至其 C&C 伺服器。該駭客集團也利用 Google 服務進行命令與控制 (C&C) 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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g5
- SONAR.SuspLaunch!g226

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.Malware.2

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。

2024/08/12

DeathGrip：新出現被稱為DeathGrip勒索軟體即服務(RaaS)的威脅集團

在不斷擴大的勒索軟體威脅版圖中，新出現被稱為 DeathGrip 勒索軟體即服務 (Ransomware-as-a-Service：RaaS) 的威脅集團。DeathGrip RaaS 透過 Telegram 和其他地下論壇進行宣傳，為暗網中雄心勃勃的威脅份子提供先進的勒索軟體工具，包括 LockBit 3.0 和 Chaos builders。他們使用被洩露的勒索軟體建置程式所建立的有效酬載，已經在網際網路上攻擊中被觀察到，讓具備最低限度專業技術的個人也能部署完全開發好的勒索軟體攻擊。

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-CPE!g2
- ACM.Ps-Http!g2
- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.Ransom!gen14
- SONAR.Ransom!gen82
- SONAR.Ransom!gen113
- SONAR.SuspBeh!gen821
- SONAR.SuspBeh!gen625
- 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：

- Ransom.Lockbit!g6
- Ransom.Zombie
- Trojan Horse
- Trojan.Gen.MBT
- Web.Reputation.1
- 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!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: Suspicious Process Accessing Lets Encrypt Certified Site
- 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。

2024/08/12

偽裝成澳洲稅務局(ATO：Australian Taxation Office)電子郵件通知的釣魚活動

澳洲稅務局 (ATO) 是澳洲政府的稅收機關。最近，賽門鐵克發現有人假冒 ATO 進行網路釣魚，誘使使用者開啟偽造的通知郵件。該電子郵件提到，由於正在進行定期維護，通知使用者需要立即注意。這些詐騙郵件目的在誘騙使用者點擊釣魚網頁。當受害者點選電子郵件內容中的釣魚網址後，就會進入憑證收集的詐騙網頁。

電子郵件主旨：

- 電子郵件主旨：1 New Important MYGov Message-Portal ID-[隨機數字字串]_
- 電子郵件寄件者："AustralianTaxationNotification" <偽造的寄件者郵件帳號> (澳洲稅務通知)

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。

2024/08/12

CVE-2024-40628／CVE-2024-40629--存在JumpServer的檔案讀取與上傳漏洞

CVE-2024-40628 和 CVE-2024-40629 是最近揭露存在 JumpServer Ansible 模組的檔案讀取和上傳漏洞。成功開採濫用此漏洞可能允許低權限帳戶存取 Celery 容器中的讀／寫檔案，造成敏感資訊洩露的風險，以及在受影響應用程式的上下文中執行任意程式碼之潛在風險。

網路知識：JumpServer 是一套開源解決方案幫助企業以更安全的方式管控和登錄各種類型的資產，允許使用者通過堡壘主機安全地訪問目標伺服器，而無需直接連接到目標伺服器。這種方法可以提高網路安全性，減少潛在的攻擊面，確保敏感數據的保密性。此拓展在 JumpServer 基礎上拓展 Ansible 的集成，可在 JumpServer 管理的資產下執行 Ansible PlayBook。

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: JumpServer Ansible Playbook CVE-2024-40628
- Web Attack: JumpServer Ansible Playbook CVE-2024-40629

2024/08/12

網路釣客以繳稅通知／繳稅證明為幌子在南韓發動釣魚行動

賽門鐵克發現一個針對韓國使用者的網路釣魚行動。該攻擊企圖冒充主要的帳戶公司發送繳稅通知／繳稅證明，以誘使收件人打開附件。附件檔案很可能是為了欺騙受害者而與韓國國家稅務局的名稱相同，即「NTS_eTaxInvoice.html」。

範例主題：

전자세금계산서(Y&S)->회계법인)

【전자 영수증】받은 새 전자 영수증[영수증 번호:]

전자세금계산서(Y&S)->회계법인하나로) 새창에서 읽기

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.Html!gen7
- Scr.Phish!gen7

基於機器學習的防禦技術：

- Heur.AdvML.B

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**。