保安資訊--本周(台灣時間2024/11/08)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 41 萬 3,300 台受保護端點上總共阻止了 4,950 萬次攻擊。這些攻擊中有 80.8% 在感染階段前就被有效阻止：**(2024/11/04)**

- 在**8萬6,900**台端點上，阻止了**1,530**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬2,800**台端點上，阻止了**810**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬9,800**台**Windows**伺服主機上，阻止了**7萬9,000**次攻擊。
- 在**5萬4,200**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,300**台端點上，阻止了**83萬1,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬8,000**台端點上，阻止了**300**萬次嘗試利用的應用程式漏洞。
- 在**12萬3,800**台端點上，阻止了**280**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,000**台端點上，阻止了**100**萬次加密貨幣挖礦攻擊。
- 在**10**萬台端點上，阻止了**860**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**529**台端點上，阻止了**8萬9,700**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 18 萬 6,600 個受保護端點上阻止了總計 780 萬次攻擊。**(2024/11/04)**

- 使用網頁信譽情資，在 **178K** 個端點上阻止 **730** 萬次攻擊。
- 攔截 **20.9K** 個端點上 **287.2K** 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 **8.3K** 個端點上攔截 **141.2K** 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 **510** 個端點上攔截 **7.5K** 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。

2024/11/07

CVE-2024-8963--存在Ivanti旗下雲端服務應用平臺Cloud Services Appliance(CSA)的路徑遍歷漏洞

CVE-2024-8963 是 Ivanti 旗下雲端服務應用平臺 Cloud Services Appliance(CSA) 的一個嚴重等級 (CVSS風險評分：9.4) 路徑遍歷漏洞，CSA 是一個透過網際網路提供安全通訊和功能的網際網路裝置。如果被成功開採濫用，此漏洞將允許未認證的遠端攻擊者存取裝置內受限制之功能。此問題會影響 4.6 Patch 519 之前的裝置版本。賽門鐵克端點防護／端點安全上的網路層防護技術：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: Ivanti CSA Path Traversal CVE-2024-8963

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，預設鎖定政策就可保護底層伺服器免受此漏洞影響，包括防止執行任意指令和限制讀取關鍵作業系統檔案。
- DCS 的網路規則政策可設定為，將應用程式限制為受信任的用戶端。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/11/07

CVE-2024-51567--存在伺服器管理主控臺：CyberPanel中的遠端程式碼執行(RCE)漏洞

CVE-2024-51567 是存在 CyberPanel 中的嚴重等級 (CVSS 風險評分：10.0／滿分) 遠端程式碼執行 (RCE) 漏洞。CyberPanel 是 Linux 伺服器的免費開放源始碼控制面板，設計用來簡化網站代管及伺服器管理任務。若成功開採濫用此漏洞，遠端攻擊者可繞過認證，並在受影響的系統上執行任意指令。此問題影響 CyberPanel 2.3.6 及2.3.7 (未修補) 之前的版本。賽門鐵克端點防護／端點安全上的網路層防護技術：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。

網路上的知識：CyberPanel 是 OpenLiteSpeed Web Server 的免費開源控制面板／伺服器管理主控臺。

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: CyberPanel Command Injection CVE-2024-51567

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，可針對此漏洞提供零時差保護。UNIX 強化政策預設會鎖定 root 帳戶，以防止管理存取權限被濫用。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/11/06

Venture Wolf駭客組織散佈RedLine惡意竊密程式的C#程式語言分支版本：MetaStealer

根據最近的報導，一個名為 Venture Wolf 的駭客組織在其最新的攻擊行動中散佈 MetaStealer 惡意軟體。攻擊鏈包括惡意檔案中包含的惡意軟體載入程式，以及以圖片、pdf 檔案或 MS Office 檔案形式的各種誘餌。MetaStealer 是 RedLine 惡意竊密程式的 C# 程式語言分支版本，具有從受攻擊電腦收集多元資訊的功能，包括：硬體和作業系統資訊、憑證、儲存在網頁瀏覽器中的資料、加密貨幣錢包、來自第三方應用程式 (例如：Thunderbird、Steam、Filezilla) 資料等。Venture Wolf 駭客組織利用 .NET Reactor 程式碼保護系統，來混淆惡意程式碼來防止逆向工程。

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

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
- 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
- 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。

2024/11/06

攻擊者利用遊戲作為誘餌散佈Winos4.0惡意軟體框架

惡意軟體框架常被威脅份子用來發動網路攻擊行動。駭客圈著名的惡意軟體框架包括 Cobalt Strike 和 Metasploit。Winos4.0 是另一個此類框架，Fortinet 已公佈最近觀察到的活動。

Fortinet 的報告中詳述的攻擊活動指出，遊戲相關應用程式是 Winos4.0 發佈的誘餌。透過相關應用程式入侵會導致多階段攻擊。第一階段是惡意的 dll，第二階段是 shellcode 的注入。第三階段是下載 dll 模組。最後階段包括下載後門的 dll 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.Ps-RgPst!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。

Carbon Black App Control 可針對此威脅提供 0-day 保護，預設配置為 Medium 或 High enforcement。

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

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。

2024/11/06

ToxicPanda：使用裝置上詐騙(ODF)技術的進化型銀行木馬程式

一種名為 ToxicPanda 全新安卓平台上的手機／行動裝置銀行木馬程式已被發現，目標是歐洲和拉丁美洲的使用者。此惡意軟體使用裝置上詐騙 (On-Device Fraud，ODF) 技術執行帳戶接管，讓攻擊者能夠繞過認證、攔截一次性密碼，並要求用戶啟用無障礙服務來啟動未經授權的交易。目前，ToxicPanda 正在積極開發中，它與 TgToxic 惡意軟體家族有相似之處，據信是由一個說中文的威脅份子所運籌。

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。

2024/11/06

Jason遠端存取木馬

Jason RAT(Remote Access Trojan) 是一種全新的遠端存取木馬，最近在地下論壇上被發現。該惡意軟體具有多種遠端存取和控制功能，包括進程、檔案和機碼控制、遠端 shell 和 PowerShell 執行等。Jason RAT 還包含額外的資訊竊取功能，專門竊取各種資料，例如：憑證、加密錢包、銀行詳細資料、cookie 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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspLaunch!g266

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!gdn32
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.2

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

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: Bad Reputation Application Network Activity
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 595
- System Infected: Trojan.Backdoor Activity 654
- Web Attack: Webpulse Bad Reputation Domain Request

2024/11/05

全新且更隱匿的惡意竊密程式～Strela Stealer

Strela Stealer 是一種新發現的惡意竊密程式，主要功能可以滲出敏感的電子郵件和組態詳細資料，例如：伺服器資訊、使用者帳號和密碼。 Strela Stealer 涉入最近頻繁行動主要是針對歐洲中部和西南部的使用者，包括德國和西班牙。初始攻擊始於含有.zip 附件的魚叉式釣魚電子郵件，類似最近購買產品的發票。在 .ZIP 壓縮檔中，可以找到嚴重混淆的 JavaScript 以及 base64 編碼的 PowerShell 指令，這些指令會連接到 WebDAV 伺服器以執行惡意 DLL。

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
- ACM.Wscr-Ps!g1
- ACM.Ps-Enc!g1
- ACM.Wscr-Net!g1
- ACM.Ps-Net!g1
- ACM.Ps-Rd32!g1
- ACM.Wscr-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：

- CL.Downloader!gen205
- JS.Downloader
- Scr.Heuristic!gen8
- Scr.Heuristic!gen22
- Scr.Malcode!gen
- Scr.Malcode!gen130
- 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!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。

2024/11/05
防護亮點：好工具淪為壞凶器又一起， AutoIt淪為駭客圈愛用的混淆器

AutoIt 是一種免費的腳本語言，設計用來自動化 Windows 圖形化介面程式和常用的腳本。自 2004 年推出第一個公開可用的版本以來，只要花點時間就可以在黑帽駭客社群找出如何濫用它的知識與經驗分享。多年來，攻擊者在攻擊鏈中多利用它來逃避偵測。

以最近的實際案例來說，在Snake Keylogger這支惡意竊密程式所涉入的惡意活動中，AutoIt就被用作混淆器。Snake Keylogger 內嵌於 AutoIt 腳本中，並由 AutoIt 腳本的編譯器 Aut2Exe 轉換為 Windows 可執行檔。

網路上的知識:混淆器是一種能將原始程式碼的功能完全保留並發揮，但令人難以閱讀與理解的工具。在特定情況，你需要提供程式給其他人，或公開在網站，例如網頁內的javascript code，基於保護個人智慧財產，你不希望別人了解你的程式邏輯與演算法，但是程式又可以必須可以正確執行。混淆器在網路攻擊中也扮演愈來越重要的角色，它能讓駭客利用現成的惡意軟體，經由混淆後，讓基於簽名檔的安全軟體，束手無策。

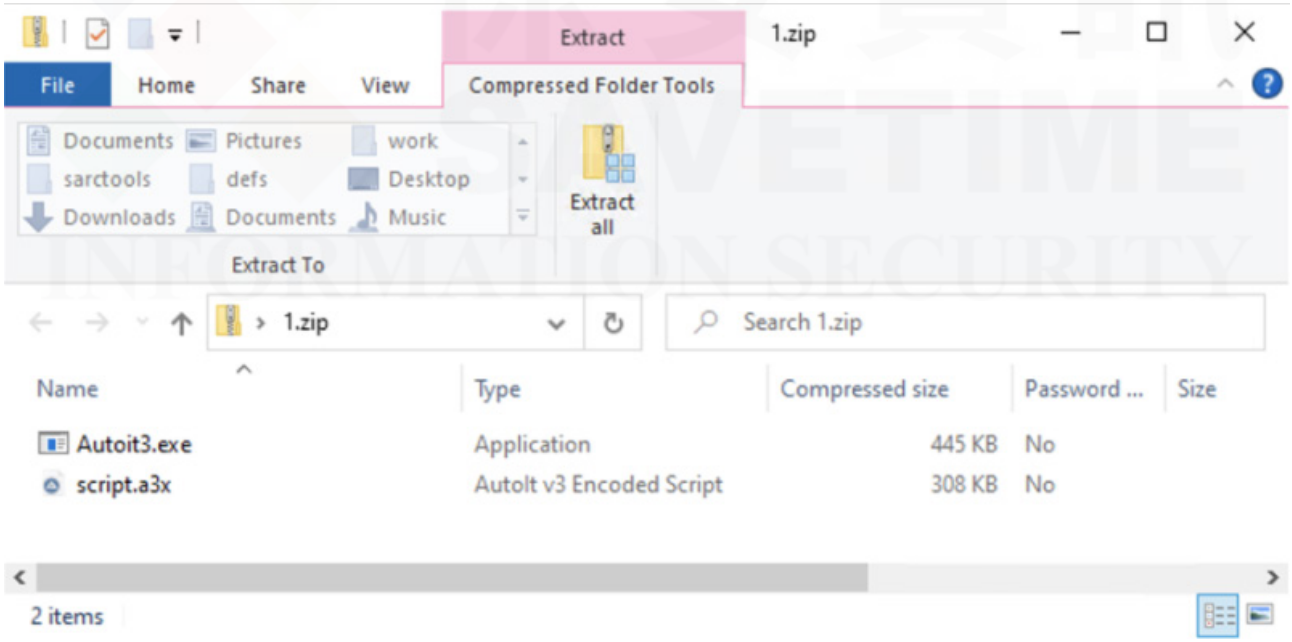
從 Windows 可執行檔中的 AutoIt 腳本編譯的二進位資料

```
A3 48 4B BE 98 6C 4A A9 99 4C 53 0A 86 D6 48 7D  .HK..lJ..LS...H}
41 55 33 21 45 41 30 36 FA E2 B0 E0 8F 64 BB AE  AU3!EA06.....d..
13 21 39 71 51 FF D6 12 6B 43 CA 52 AF AD 00 00  .!9qQ...kC.R....
E6 FB 25 78 C8 E2 13 F9 7D 1D ED DD 71 00 B0 55  ..%x....}...q..U
2D AC 9A D5 28 15 D4 F0 CF 25 E4 CF 11 8E 56 C2  -...(....%....V.
CE 3F 70 EF B9 68 12 F8 00 00 2E AC 66 00 E7 CE  .?p..h......f...
36 AE 6B 99 3D 58 92 51 E9 53 69 0C 1A 2E 52 00  6.k.=X.Q.Si...R.
5D C1 C8 FC 3A D8 F7 B6 0B 1E 6A 14 46 AE 55 80  ]...:.....j.F.U.
58 FF 58 DE AF 8B 98 A1 80 91 5A 52 F1 5D 9A 94  X.X.......ZR.]..
1F 01 A6 6B 1C 48 4E 8D E3 D3 64 DD 93 F0 08 85  ...k.HN...d.....
A8 52 5B E7 10 77 B8 98 5D 4A 40 46 C2 91 8A A3  .R[..w..]J@F....
B4 98 9D C5 9D 88 71 3D 17 F8 D0 33 67 A0 01 0E  ......q=...3g...
EF 09 00 65 D6 1C 00 FE 9A 21 50 96 0A DB 01 61  ...e.....!P....a
22 22 A0 96 0A DB 01 E3 AB 2B A0 6D FB FA 03 B3  "".......+.m....
97 6F 60 85 F2 38 8E 35 E6 DE 0C 78 D2 E3 F2 28  .o`..8.5...x...(
6E 55 8B 6A 84 F5 A4 00 30 36 A8 6E 22 B7 51 02  nU.j....06.n".Q.
```

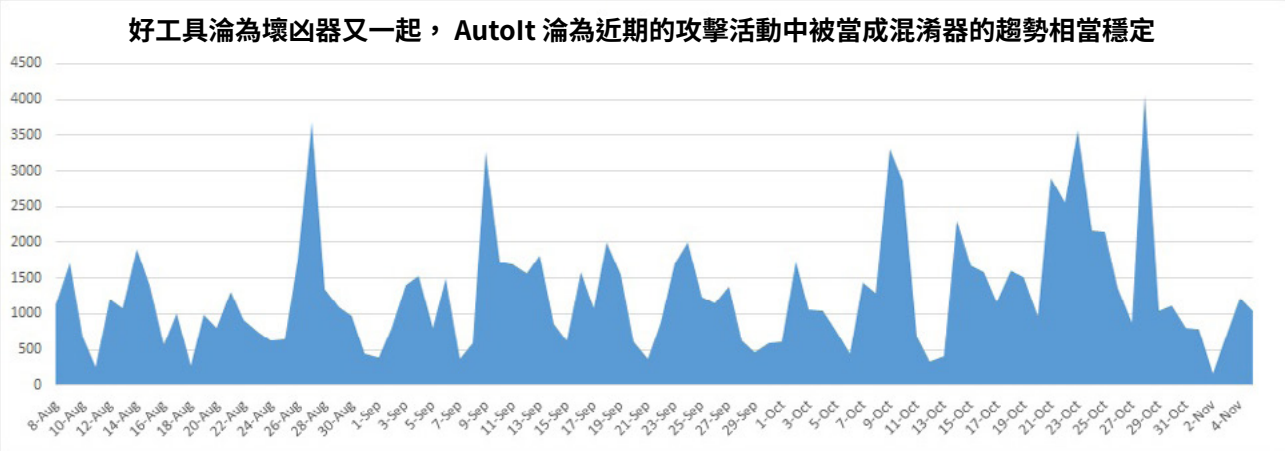
從編譯資料中提取的 (混淆) 腳本

```
Global $xvqmwba = "0x1b00d44951594f5842535249b0c64a41f75932584a5755560a4230524750565a444952594f58465352494f394a414f5932584a5755
$xvqmwba &= "932384e5759564a4230524750565a444952594f58465352494f394a414f5932584a5755564a4230524750565a444952594f58465352494f394
$xvqmwba &= "20150565a0449525978584653774944f3927414f5916584a572b564a424e524750325a444920594f582753524908394a412059325824575556
$xvqmwba &= "52623e55564c421a68472e4a5a444d5036a35846597463e13934064f59362602575552347b30524322c24444397a114f584c21c8574f496291
$xvqmwba &= "e65a444d7959657a44502ff94f394e6b695b49e94a57517d4a681250442de75a444d787f4d23f453524d643960634d5a4fea4a57517c6c404b
$xvqmwba &= "4220524750575a44585274e5846573d6e4f39404b64593472596754565a4230524550564b443750594f5c297b52494533614149732168 4b57
$xvqmwba &= "d43524b402667594f5252ad515a4a284f57b15acc496c256e564a3227df0750565b615f435d206d4653582679394a4bed711d584a5d46505b4
$xvqmwba &= "94a41435932494a296a564a48bc5a47504d4eba48595e63526e51524964b975414f534c674a575f5c6142367847504564a46496e594f584b535
$xvqmwba &= "52475656290149525367744653544493c7c4a4145711c584a5155250f4230586f60565a4249211c4f584c7b60494f3f4a320a593252626355564
$xvqmwba &= "055846597a104f394c690559325238105656 3a6a7a52475a24f9474922710558465 97a114f394c690559325238105656 3a6a7a52475a24e547
$xvqmwba &= "55640c2095247542403404922276358465 77a194f394cc17559325c38e451563a3c1c5247547e0a444954d97458465720ac4b393a3f6359325
$xvqmwba &= "5f7e03423058c71b565a403b175e4f28c61e52494b4b21464f29b2004a57517c597232527350565a544952485ba6403552494944a1a414f5338
$xvqmwba &= "7545d5d684e555f200a465358635c0948417b5932585a5755475ebc362c4750502914495253452654535 24d443e6646485f5d094a575f54ca5
$xvqmwba &= "9b34a41492a62584a5d5f285c4230564c577a5d434f3d084f584c51d25f4f394e3f5959325c415079514d445f0047505c70577950597b584653
$xvqmwba &= "59434020654a41454a38494e4650405b47be3b280e565a4e49435d5e52504258c7265614414f53322a435e552650cf33524751734c40eb774e
$xvqmwba &= "de5946535c494f394a414f5930584a57f8574a422b5247509e5b44495c594f58465352494f394a414e5932589d5655569243305257505 65a01
$xvqmwba &= "74a3012584720547214495 25f45734655784 94f3959714d5923584a575f564a5330203b5a562a466102594f5e4c78524f65394a4154693758e
$xvqmwba &= "85a492b4c33885e322862025556406a7952475a5d5c2b395259452a4e5852393dec4d413f5e1a114a575f393b42305847563928444958 5b202
$xvqmwba &= "a575f221a4230534c2e2e5a44435e594837265352434239432e3659325259534452621830524d232c5a4443415c5e5d29285249451f94374f4
$xvqmwba &= "144f57035352485 4094f41c259325852575547 4a4243d547505c5137c1525945543409534 3f3454cc1059325959535d7ec3423058443f0a5a
$xvqmwba &= "4a48429b4b5026720d4952535c5c575758624f3f60415c6931586c5755565042304347 8c05a44437ace4f584c2183454f4962d94f593870dd
$xvqmwba &= "9384b4e894573627630524d43515a6c2b5259458646534 4d3c9a4a41454a37494f382e564a4823545654 39fe444958595e5d29f6524945395
$xvqmwba &= "496945588e53524952394a504f5941ff4a575f5d38c23e523778005a444f7a124f584c5f555d3dfb44413f4ebf5b4a5754735c4a92775455424
$xvqmwba &= "2d594f59634545d56a2a4c5667f13258407144505cd31d506c5a475f52d37a624f584c5f553bb5374a3120f03258405a270c4b4240414359391
$xvqmwba &= "7422d9c52475a455e44585536e258465941405e30679a914e235f3f4255564b6e3d434025435a44483d584f584c538e584b3394536a7106584
$xvqmwba &= "4928397bd94f4e32584a5755564b4283e64742135a4448496945588e53524952394a504f5941ff4a575f5d38c23e523778005a444f7a124f58
```

在另一個案例中，DarkGate 涉入攻擊活動的攻擊鏈中使用了 AutoIt。一個包含合法 AutoIt 解譯器 Autoit3.exe 和惡意編譯的 AutoIt 二進位檔 script.a3x 的 Zip 檔案被放置在受攻擊的網站上。攻擊鏈的前一階段會下載 Zip 檔案，解壓後並執行含有惡意二進位檔的 Autoit3.exe。



在這兩種情況下，攻擊者都會將惡意程式碼隱藏在 AutoIt 腳本中，以增加偵測的難度。我們長期對此攻擊手法與途徑的持續監控顯示其趨勢相當穩定。



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：

- AUT.Heuristic!gen1
- AUT.Heuristic!gen3
- AUT.Heuristic!gen5
- AUT.Heuristic!gen6
- AUT.Heuristic!gen7
- AUT.Heuristic!gen10
- AUT.Heuristic!gen12
- AUT.Heuristic!gen13
- AUT.Heuristic!gen14
- AUT.Heuristic!gen15
- AUT.Heuristic!gen16
- AUT.Heuristic!gen18
- AUT.Heuristic!gen19
- AUT.Heuristic!gen20
- AUT.Heuristic!gen22
- AUT.VictoryGate!gen1
- Scr.Malscript!gen14
- Scr.Malcode!gen

賽門鐵克提供三種常見情境的端點安全解決方案：SEP／SESE／SESC，請點擊此處了解解決方案的全貌以及您的企業適合選用哪一種方案。

在重要的伺服主機，例如：AD、SQL、ERP、WEB、Exchenge……主機，賽門鐵克基於政策強制、最低資源、最少權限及網路入侵防禦技術……DCS：Data Center Security 是大型企業列為資料中心必要的解決方案，請點擊此處瀏覽 DCS 的完整資訊。

2024/11/05

Amnesia Stealer惡意竊密程式

Amnesia 是在真實網路情境中被發現的大眾化惡意竊密程式。其原始碼已被公開，並將建置程式碼發佈在 GitHub 上，好讓各路人馬都能輕易取得。Amnesia 具備多種功能，包括鍵盤側錄、加密和一般資訊竊取。惡意竊密程式的目標是遭入侵機器上的敏感資料，例如：憑證、cookies、瀏覽器 session 檔案、cryptowallets、無線網路憑證、Discord 權杖、遊戲 session 資料等。惡意軟體利用 Discord 和 Telegram 進行 C&C 網路通訊。

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-RgPst!g1
- ACM.Ps-Schtsk!g1
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g266
- SONAR.SuspLoad!gen2

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
- ISB.Malscript!gen25
- Scr.Malcode!gdn32
- Scr.Malcode!gen129
- Trojan.Gen.MBT
- 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：

- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 568
- System Infected: Trojan.Backdoor Activity 656

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。

2024/11/05

CVE-2024-9264--存在圖像化資料分析系統Grafana中的嚴重等級漏洞

CVE-2024-9264 是一個最近被揭露的嚴重等級 (CVSS 風險評分：9.4) 漏洞，會影響圖像化資料分析系統 Grafana 的 QL 表達式 (SQL Expressions) 實驗性功能，Grafana 是一個開放原始碼分析與監控工具。如果成功開採濫用此漏洞，可能會導致指令注入和本機檔案包含攻擊 (LFI：Local File Inclusion)，可能會允許未經認證的攻擊者存取敏感檔案，並允許他們在有漏洞的 Grafana 實體上執行任意程式碼。減緩此漏洞的修補軟體版本已經發佈。

網路上的知識：LFI 全稱 Local File Inclusion，從字面上就可以大致理解這種攻擊手法，簡單來說就是攻擊者利用網站上某些會引入Server 本地端的文件 (檔案)，而去訪問敏感 (或預期外) 檔案的攻擊手法。

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：

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: Grafana CVE-2024-9264

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 的 IPS 阻擋政策可以控制哪些程式可以在自訂 Grafana 沙箱中執行。它也可以控制哪些資源可以寫入或讀取。保安資訊補充說明：在 DCS 的情境中出現的自訂沙箱，原則上是指剛剛好可以讓應用程式可以運行的環境，限縮的權限、限縮的資源、不同程序間的呼叫、限縮的網路存取……，把這些環境參數變成強制的政策，即便遭入侵，被植入惡意程式 (根本不可能被植入，也不可被入侵)，因惡意程式沒有運行的空間，所以整個系統是安全的。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/11/05

最近在真實網路情境出現的全新惡意軟體：WrnRAT

WrnRAT 是最近在真實網路情境出現的全新惡意軟體。此惡意軟體的植入程式透過偽裝成熱門賭博遊戲網頁的網站散佈。WrnRAT 是一個採用 Python 開發的惡意軟體，其功能包括收集系統資訊、收集螢幕截圖、竊取受害者的敏感資訊或允許攻擊者遠端存取受攻擊的機器。進一步入侵還可能允許傳送和執行其他任意的有效酬載。

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

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.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/11/04

台灣的Facebook商業用戶請留意～LummaC2和Rhadamanthys惡意竊密程式活躍在最近攻擊行動中

根據 Cisco Talos 最新報告，LummaC2 和 Rhadamanthys 惡意竊密程式已在最近觀察到的惡意攻擊行動被發現。在這次攻擊中散佈的網路釣魚電子郵件利用「版權侵犯問題」為誘餌，以台灣的 Facebook 商業用戶為目標。攻擊者也濫用 Dropbox 和 Google 的 Appspot.com 網域，將惡意 .RAR 壓縮散佈給毫無戒心的受害者。開啟下載的檔案後，使用者會收到以虛假 PDF 執行檔形式傳送的惡意有效酬載。LummaC2 和 Rhadamanthys 都是知名的惡意竊密程式，在威脅領域中早已存在，其目標是從被攻擊的系統中竊取機密資訊。

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
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspBeh!gen530
- 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.MBT
- 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。

2024/11/01

破解EDR防禦逃脫工具揭發威脅者在攻擊鏈所採用的駭客工具組合

EDR (端點偵測與回應) 防禦逃脫工具透過中斷安全產品與系統的連結 (與系統脫鉤)，協助隱藏惡意活動。在 Palo Alto Networks Unit 42 發表的一份報告中，他們提供一宗事件的分析，在該事件中，研究人員發現 EDR 防禦逃脫 (Defense Evasion) 工具，並藉此發現威脅者的特定識別特徵。該事件顯現出典型的攻擊技術 (橫向移動 (Lateral movement)、探索 (Discovery)、持續性 (Persistence)、滲出 (Exfiltration)等)，最終目的是勒索。分析還發現其他工具，例如：易受攻擊的驅動程式、Rclone 和 portscanners 等兩用工具，以及其他已知的惡意軟體，例如：Mimikatz 和 Cobalt Strike。

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.Rcln-Lnch!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g30

- SONAR.SuspDriver!g40
- SONAR.SuspLaunch!g138
- SONAR.SuspLaunch!g445
- 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：

- Hacktool.Rebeus
- Hacktool.Rebeus!gen1
- Hacktool.SharpHound
- Trojan Horse

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

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。

2024/11/01

Stonefly進階持續威脅(APT)駭客組織參與傳播Play勒索軟體的行動

網路威脅聯盟 (Cyber Threat Alliance，CTA) 會員 Palo Alto Networks 最近一份報告揭露 Stonefly (又名 Jumpy Pisces、Andariel) 駭客組織如何與一個名為 Fiddling Scorpius 的 Play 勒索軟體攻擊者合作，一改以往利用客製化勒索軟體的策略。在這次最新的攻擊中，攻擊者透過遭入侵的帳戶取得存取權，讓他們可以部署各種惡意軟體和工具。一旦部署完成，他們就可以橫向移動並進一步升級攻擊，最終達成 Play 勒索軟體的傳播。

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：

- Backdoor.Preft
- Hacktool.Gen
- WS.Malware.1

基於機器學習的防禦技術：

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

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。

2024/11/01

惡意廣告行動使用Latrodectus惡意程式下載器，散布滲透測試工具Brute Ratel C4有效酬載

EclecticIQ 威脅研究團隊報告一個與進階持續威脅 (APT) 駭客組織：Blister(又名 Lunar Spider)有關聯的全新惡意廣告攻擊行動。攻擊者利用 Latrodectus 惡意程式下載器，散布滲透測試工具 Brute Ratel C4 有效酬載。在 Bing 瀏覽器上搜尋稅務相關內容的使用者會被引誘下載混淆的 JavaScript。執行後，這個腳本會從遠端伺服器擷取 Windows 安裝程式 (MSI)，安裝 Brute Ratel 惡意軟體。此惡意軟體隨後會連線至指令與控制 (C&C) 伺服器以取得進一步指示，讓攻擊者控制受感染的系統。

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-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：

- ISB.Downloader!gen195
- Scr.Malcode!gen
- Trojan.Latrodectus!g1
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Reputation.1

基於機器學習的防禦技術：

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

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**。