保安資訊--本周(台灣時間2024/12/27)
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 37 萬 3,900 台受保護端點上總共阻止了 4,410 萬次攻擊。這些攻擊中有 77.2% 在感染階段前就被有效阻止：**(2024/12/23)**

- 在**8萬3,200**台端點上，阻止了**1310萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬3,900**台端點上，阻止了**720萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬6,800**台**Windows**伺服主機上，阻止了**6萬6,000**次攻擊。
- 在**5萬1,500**台端點上，阻止了**170萬**次嘗試掃描伺服器漏洞。
- 在**1萬1,900**台端點上，阻止了**82萬3,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬6,100**台端點上，阻止了**220萬**次嘗試利用的應用程式漏洞。
- 在**8萬1,500**台端點上，阻止了**150萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,700**台端點上，阻止了**89萬6,000**次加密貨幣挖礦攻擊。
- 在**10萬2,500**台端點上，阻止了**930萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**449**台端點上，阻止了**7萬8,700**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 19 萬 1,500 個受保護端點上阻止了總計 690 萬次攻擊。**(2024/12/16)**

- 使用網頁信譽情資，在 **182.3K** 個端點上阻止 **650** 萬次攻擊。
- 攔截 **19.6K** 個端點上 **250.9K** 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 **8.2K** 個端點上攔截 **170.1K** 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 **250** 個端點上攔截 **6.1K** 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。

2024/12/25

Gosar--採用Golang語言撰寫Quasar後門程式的最新變種

Gosar 是最近發現採用 Golang 語言撰寫的 Quasar 後門程式最新變種。該惡意軟體利用偽裝成合法軟體安裝包 (例如：Telegram 或 Opera) 的 .MSI 安裝程式檔案進行傳播。攻擊者利用被稱為 SadBridge 的全新惡意程式載入器，採用 DLL 側載技倆進行有效酬載的注入與執行。部署的 Gosar 有效酬載是一個多平台後門，包含各種功能，例如：從受攻擊的端點收集資訊、執行指令、擷取畫面、啟動 HVNC 會話、擷取檔案等。

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.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：

- Trojan Horse

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.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。

2024/12/24

防護亮點：賽門鐵克重要主機防護系統--Data Center Security(DCS)的安全強化機制，保障系統管理員的合法好工具不會淪為勒索軟體攻擊中之壞凶器

資料中心遭勒索軟體攻擊越來越普遍

勒索軟體是當今網路安全的最大威脅之一，每年都以驚人的速度增長。從個人、小型政府機構到全球化的大型組織，無一能倖免。由於其對地緣政治目標、企業業務系統和關鍵公共基礎設施造成前所未有的損害，勒索軟體現在被歸類為網路恐怖主義。勒索軟體攻擊者以多種不同的方式策劃他們的攻擊，並利用基礎架構中已有的多種工具或在攻擊期間下載的各式工具。這些工具在其自身的使用場景中通常是合法的，並被管理員廣泛使用。但當這些工具在攻擊情境中被威脅行為者濫用時，它們就會變得具有破壞性，並可能造成極大的損害。只需突破一個端點，攻擊者就可以利用合適的工具存取多個互有關聯的系統和應用程式，其潛在的風險說多大就有多大。

為了防禦勒索軟體，企業組織需要採取完整而全面、全員參與、縱深防禦的方式，充分利用整個組織的資源。

Data Center Security--重要主機最有效的防護解決方案

賽門鐵克的重要主機防護系統：Data Center Security(DCS) 提供完整而全面縱深防禦的方式，以保護和保障 IT 基礎結構和連線端點的安全。我們的解決方案在提供針對日益增加的某些流行合法工具在勒索軟體攻擊和其他類型網路犯罪中使用的零日保護方面非常有效。

勒索軟體攻擊中常見的使用的工具

在本節中，我們將探討一些在勒索軟體攻擊中常被濫用的合法工具及 DCS 如何防禦它們。

- **Cobalt Strike**：一種現成的工具，可用於執行指令、注入其他程序、提升目前程序或冒充其他程序，以及上傳和下載檔案。表面上，它有合法的用途，可作為滲透測試工具，但終究遭惡意行為者濫用。目前被 Clop、Conti、DoppelPaymer、Egregor、Hello(WickrMe)、Nefilim、NetWalker、ProLock、RansomExx、Ryuk 等勒索軟體家族大肆濫用。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會鎖定端點網路，以減少其攻擊面。預防政策中「Suspicious Process Execution」等規則可防止 Cobalt Strike 注入程式／beacon 在系統上注入或執行。也可以阻止資料外洩。程序存取控制 (Process Access Control) 可保護所有系統程序，防止非法注入、冒充或提升權限。

- **Mimikatz**：用於憑證轉存的漏洞利用工具。目前被 DoppelPaymer、Nefilim、NetWalker、Maze、ProLock、RansomExx、Sodinokibi 等勒索軟體家族大肆濫用。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止此工具執行。該政策將限制 Mimikatz 取得 LSASS 或 LSA 等程序的轉存，以竊取憑證。

- **PsExec**：用於在遠端系統中執行程序。在勒索軟體攻擊中，它通常用於執行任意指令 shell 和橫向移動。幾乎所有現存的勒索軟體家族都會使用它。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策預設會阻止 PsExec 執行。

- **AnyDesk**：合法的遠端桌面應用程式。透過安裝它，攻擊者可以遠端存取網路中的電腦。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止系統使用任何遠端桌面功能。任何人都無法從系統存取 RDP。

- **ADFind**：可用於從活動目錄 (AD) 收集資訊的免費工具。AdFind 可以查詢 AD 中的電腦、識別網域使用者和網域群組、從 AD 中提取子網路資訊。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止該工具的執行。它也會阻止查詢 AD 的任何資訊。

- **RDP**：遠端桌面通訊協定 (Remote Desktop Protocol)。微軟開發的通訊協定，允許電腦使用用戶端／伺服器軟體，連線並控制另一台電腦。攻擊者可嘗試使用各種技術啟用 RDP，包括利用多種就地取材 (LOTL) 工具。一旦啟用 RDP，就會讓攻擊者利用 RDP 通訊協定的任何兩用工具。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會阻止系統使用任何遠端桌面功能。任何人都無法從系統存取 RDP。

- **WinRAR／WinSCP**：可用於封存或「壓縮」檔案的壓縮檔管理程式。攻擊者使用 WinRAR 和類似的工具 (例如：7-Zip) 來準備檔案以進行外洩。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會鎖定網路，因此會封鎖任何入埠或離埠的 ftp 連線。

- **PowerShell**：一種微軟指令碼工具，可用於執行指令、下載有效酬載、遍歷受攻擊網路以及進行偵查。在數次的勒索軟體攻擊中，攻擊者執行特定指令進行資料外洩，包括使用 Compress-Archive cmdlet。

DCS 已內建重要主機常見使用情境的防禦政策集 (default prevention policies)，套用該防禦政策會防止針對「受攻擊」(例如：IIS Worker) 程序在攻擊鏈的任何階段，以程序譜系啟動任意 cmd 和 PowerShell。

- **多種工具**：有些攻擊行動會同時使用多種工具，而非只使用單一工具，因為一種工具可用來啟用另一種工具。例如：可被濫用來竊取憑證的 Mimikatz 可以允許存取需要管理員權限的 PsExec 功能。勒索軟體 Nefilim 涉入的攻擊行動同時會使用多種工具，它使用 AdFind、Cobalt Strike、Mimikatz、Process Hacker、PsExec 和 MegaSync 等工具。

DCS 已內建常見使用情境的防禦政策集 (default prevention policies) 套用該防禦政策會將系統程序置於獨立的沙箱中，以防止它們受到外部工具的攻擊。此外，管理員帳戶會被鎖定，以防止任何工具嘗試將自己提權為管理員權限。

DCS 的安全強化機制，保障兩用工具沒有被濫用的空間

DCS 的安全強化提供作業系統和應用程式程序運行所需剛剛好的沙箱控制、網路、檔案系統、登錄檔、程序間記憶體的存取、系統呼叫，以及應用程式和子程序啟動的細部存取控制。這些強化能力可有效限制上述攻擊情境中使用的工具，使其只能用於合法用途，進而讓攻擊無效。

欲了解有關賽門鐵克的重要主機防護系統：Data Center Security(DCS) 更多資訊，請點擊此處。

2024/12/24

新一波XWorm惡意軟體散佈行動，鎖定餐旅行業為攻擊目標

據報導，一個散佈商業化惡意軟體：XWorm 的全新攻擊行動已在真實網路情境中發動。攻擊目標是英國的餐旅行業。惡意軟體透過含有惡意網頁的釣魚電子郵件散佈，依附在這些惡意網頁上的 PowerShell 腳本會在隨後攻擊階段中成為幫凶。此攻擊行動中惡意垃圾郵件偽裝成來自 Booking.com 旅遊平台的詐騙訊息。XWorm 是一種知名的惡意軟體，通常以惡意軟體即服務 (MaaS) 的形式銷售。它具有多種功能，包括鍵盤側錄、資訊竊取、下載其他的任意有效酬載、遠端存取木馬 (RAT) 等惡意功能。

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-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.RegRun-TMshta!g1
- ACM.Untrst-RgPst!g1
- 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。

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!gen10
- ISB.Downloader!gen76
- Trojan.Gen.2
- 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!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。

2024/12/24

最新I2PRAT惡意軟體後繼新變種，利用匿名點對點網路通訊

最新 I2PRAT 惡意軟體後繼新變種已被發現到利用 I2P(Invisible Internet Project 即「隱形網際網路計劃」) 匿名點對點網路進行 C&C 通訊。I2PRAT 具備完全模組化的架構，其獨立外掛負責 I2P 連線初始化、任意檔案下載、RDP 設定、工作排程建立、使用者帳戶管理等。惡意軟體還能收集遭感染端點的各種資訊，包括網路介面卡資料的記憶體狀態、登錄機碼或儲存在該網路瀏覽器中的資訊等。

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.Ps-Rd32!g1
- ACM.Ps-Sc!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- W32.Silly!gen
- WS.Malware.1
- WS.Malware.2
- WS.Reputation.1
- WS.SecurityRisk.3

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: Trojan.Backdoor Activity 721

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。

2024/12/23

在針對泰國的網路釣魚行動中發現全新後門程式：Yokai

據報導，一個被稱為 Yokai 的全新後門程式涉入針對泰國企業的惡意軟體攻擊行動。此攻擊始於一封偽裝成美國法律部門通訊的釣魚電子郵件，其中包含一個內含兩個 .LNK 捷徑檔案的 RAR 壓縮檔附件。點擊後，LNK 檔案會引導至詐騙文件和一個安裝合法資料備援軟體：iTop Data Recovery 的惡意軟體植入器的有效酬載，同時側載 Yokai 後門。此後門可提供攻擊者遠端存取權限。

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 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

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。

2024/12/23

CoinLurker惡意軟體

據報導，網路不法份子利用假的軟體更新當誘餌，傳送一種名為 CoinLurker 的全新惡意竊密程式。這種多階段攻擊利用 Microsoft Edge Webview2 以及 Binance Smart Contracts 和 Bitbucket 儲存庫隱藏其有效酬載。CoinLurker 以 Go 語言撰寫，是一款複雜的惡意竊密程式，目的在滲透敏感的使用者資料，包括加密貨幣錢包資訊、金融應用程式及其他個人資料。它採用先進的混淆和反分析技術來逃避偵測。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g221
- SONAR.SuspLaunch!g444
- SONAR.SuspPE!gen32
- SONAR.SuspStart!gen18

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：

- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.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。

2024/12/22

節日購物旺季提醒：網路不法份子盯上日本節日購物族群

日本的年終節日購物旺季橫跨十二月底至一月初，是一個重要的文化期間，包括聖誕節、除夕 (Ōmisoka)、元旦 (Shō gatsu)。聖誕節的特色是傳統、家庭聚會、送禮和慶祝活動，因此是消費活動頻繁的期間。這種高度的活動，加上年節氣氛，讓詐騙利用情感觸發和對國產品牌的信任創造機會。在爭相獲取優惠的過程中，人們可能會忽略可疑的跡象，而假期間金融業的休息則為攻擊者提供假酬謝和假冒的付款頁面進行詐騙的空窗時間。

舉例來說，本月就有一名釣魚者試圖釣取 PayPay 用戶帳密。這些電子郵件宣傳 PayPay 的各種節日活動，提供在年底和新年假期賺取或贏取 PayPay 點數的機會。這些郵件強調盛大的抽獎活動、季節限定優惠、購物獎勵，以及與聖誕節、除夕夜和元旦有關的獨家活動。這些訊息利用節日氣氛和消費者的興奮情緒，保證從小額現金到價值數十萬日圓的獎品回饋，以可觀的獎賞吸引消費者的注意。在電子郵件中，惡意網址會將受害者重新導至偽造的 PayPay 登入頁面。

觀察到電子郵件主題清單大致如下：

- 🎊 PayPay 新年開運キャンペーン – 最大20,000円分のPayPayポイントをプレゼント 🎊
- お正月の運試し！PayPayで最大100,000円が当たる大抽選会！
- 大晦日の驚き！最大20万円分のPayPayポイントで2024年を締めくくろう
- 🎉 新年初売り！最大10,000円分のPayPayポイント還元 🎉
- 2025年新年福袋キャンペーン！お得なポイントが手に入るチャンス！
- 豪華賞金20万円があなたを待っている！今すぐ参加しよう
- PayPay ウィンターワンダーランド – 最大20万円相当ポイントが当たる！
- 🎄 クリスマス限定！最大15,000円分のPayPayポイントプレゼント 🎄
- ⏰ 年末カウントダウン！PayPayで最大50,000円分のポイントをゲット ⏰
- ✨ 年末感謝祭！最大10,000円分のPayPayポイントバック ✨
- 🎉 新春特典！最大5,000円分のPayPayポイントバック 🎉
- ❄️ 冬のショッピング祭り！最大30,000円分のPayPayポイントプレゼント ❄️
- 開運の鍵はここに！PayPayで最大12万円分のポイントチャンス

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。

2024/12/19

VIPKeyLogger惡意竊密程式涉入的威脅活動呈上升趨勢

有越來越多的威脅團體和個體戶使用 VIPKeyLogger 這個惡意竊密程式。雖然透過偷渡式下載和電子郵件傳播，但主要是後者。以下是最近在全球觀察到的惡意垃圾郵件行動中用來騙取使用者的郵件附件檔案名稱範例：

- fiyati_teklif_65w20_büyük_siparipi.pdf.exe
- request_for_quote_docs.exe
- transferencia_realizada_451.exe
- factura.exe
- payment_advice.exe
- dekont_7083037_halkbankasi.pdf.exe
- aralik_po_iron-te_160924_563028621286.pdf.exe
- quotation_august_2024.pdf.scr
- rfq_for_wika.pdf.exe
- purchase_order_abniro_bandar_imam_co.pdf.exe
- malzeme_görsel_siparipler_160924.exe

功能：

此威脅會收集各種資料，包括電腦名稱、國籍資訊、剪貼簿內容、螢幕截圖、cookie、瀏覽歷史紀錄等。它會透過 Telegram 傳送收集到的資訊。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- 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。

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：

- MSIL.Packed.43
- Trojan.Gen.2

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

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: TLS v1 Request
- Audit: Untrusted Telegram API Connection
- System Infected: Bad Reputation Application Connecting to Cloud Storage

基於機器學習的防禦技術：

- Heur.AdvML.C

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**。