保安資訊--本周(台灣時間2024/11/22)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 400 台受保護端點上總共阻止了 4,490 萬次攻擊。這些攻擊中有 78.2% 在感染階段前就被有效阻止：**(2024/11/18)**

- 在**8萬8,400**台端點上，阻止了**1,280**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬4,200**台端點上，阻止了**790**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬8,200**台**Windows**伺服主機上，阻止了**7萬3,000**次攻擊。
- 在**5萬2,600**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬100**台端點上，阻止了**67萬7,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,000**台端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在**11萬8,200**台端點上，阻止了**220**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,000**台端點上，阻止了**95萬3,900**次加密貨幣挖礦攻擊。
- 在**10萬7,100**台端點上，阻止了**890**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**503**台端點上，阻止了**7萬7,600**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 2,500 個受保護端點上阻止了總計 790 萬次攻擊。**(2024/11/18)**

- 使用網頁信譽情資，在 **183.9K** 個端點上阻止 **740** 萬次攻擊。
- 攔截 **21.2K** 個端點上 **272.7K** 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 **8.3K** 個端點上攔截 **135.8K** 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 **433** 個端點上攔截 **8.2K** 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。

2024/11/21

新版Cryptbot惡意軟體～強化後端伺服主機(C&C)連線的加密機制

Cryptbot 是一種具有資訊竊取功能的惡意軟體。它針對廣泛的敏感資料進行資料外洩，例如：瀏覽器 cookie、憑證或加密錢包。已知 Cryptbot 會透過惡意網頁或破解版軟體的安裝程式散佈。此惡意軟體的最新變種最明顯的進化是強化後端伺服主機 (C&C) 連線的加密機制。

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
- 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

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。

2024/11/20

惡意軟體劫持受信任防毒軟體廠商的驅動程式

最近一次惡意軟體攻擊行動揭露一家網路安全廠商的合法 Anti-rootkit 驅動程式被操控來執行有害動作。該惡意軟體濫用受信任的「aswArPot.sys」核心模式驅動程式，將自身安裝為服務，進而取得關鍵系統程序的存取權。這讓它可終止防毒軟體和端點偵測，繞過安全防禦，並提高對系統的控制。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspDriver!g10

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

2024/11/20

「ELPACO-team」勒索軟體～源於Mimic更隱匿、更低調的後繼新變種

研究人員最近發現一個惡意檔案，專作為部署「ELPACO-team」勒索軟體的植入程式。據觀察，這種勒索軟體是源於 Mimic 勒索軟體的後繼新變種。它能夠加密關鍵檔案、停用安全軟體的功能、為了確保其持續性／常駐能力，同時避開重要的系統檔案，讓偵測和復原變得複雜。

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.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen616
- SONAR.SuspBeh.C!gen10
- SONAR.SuspLaunch!g324

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool
- Ransom.Mimic
- Scr.Malcode!gdn32
- Trojan Horse
- WS.Malware.1
- WS.Malware.2
- 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

2024/11/20

開採濫用防火牆漏洞駭入目標環境的Helldown勒索軟體

Helldown 是最近在真實網路情境裡被發現的全新勒索軟體。此惡意軟體同時可針對 Windows 和 Linux 環境。Helldown 會加密使用者檔案，並以「ReadMe.[encrypt_extension].txt」文字檔的形式留下勒索(贖金支付)說明。攻擊者採用雙重勒索戰略，威脅受害者不就範就會公開先前加密的機密檔案。據報導，Helldown 勒索軟體的初始攻擊階段是利用現有防火牆漏洞來駭入目標環境。

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.Untrst-RunSys!g1
- ACM.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen113
- SONAR.Ransomware!g16
- SONAR.SuspBeh!gen821
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g250
- 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：

- Ransom.Helldown
- Ransom.Helldown!g1
- 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

2024/11/20

FrostyGoop又出現了～專門針對工控系統(ICS)類型的營運科技(OT)環境基礎架構的惡意軟體

根據 Palo Alto Networks 最近報告，在真實網路情境裡已經發現到 FrostyGoop (也稱為 BUSTLEBERM) 惡意軟體的新樣本。這個以 Go 語言撰寫的惡意軟體最初是在 2024 年被發現，並曾出現在針對烏克蘭重要基礎設施的攻擊型行動中。FrostyGoop 專門針對工控系統 (ICS) 類型的營運科技 (OT) 環境基礎架構，具有與受攻擊系統進行 Modbus TCP 通訊協定通訊的能力。攻擊者可能會透過可用的網際網路連線從外部或直接在已遭入侵的內部網路操弄此惡意軟體。

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：

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!500
- Heur.AdvML.C

2024/11/19

提醒：雲端會計系統QuickBooks的用戶，小心來自Google廣告詐騙

在真實網路情境裡出現一個以雲端會計系統 QuickBooks 的用戶為目標，透過 Google 廣告宣傳的騙局，假冒支援網站和惡意程式產生假的資料損毀彈出視窗。受害者會被誘騙從 Dropbox 下載合法的 QuickBooks 軟體以及隱藏的後門檔案。一旦安裝，惡意軟體就會允許詐騙者存取和竊取敏感資料，同時還會收取假的修復費用。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

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。

2024/11/19

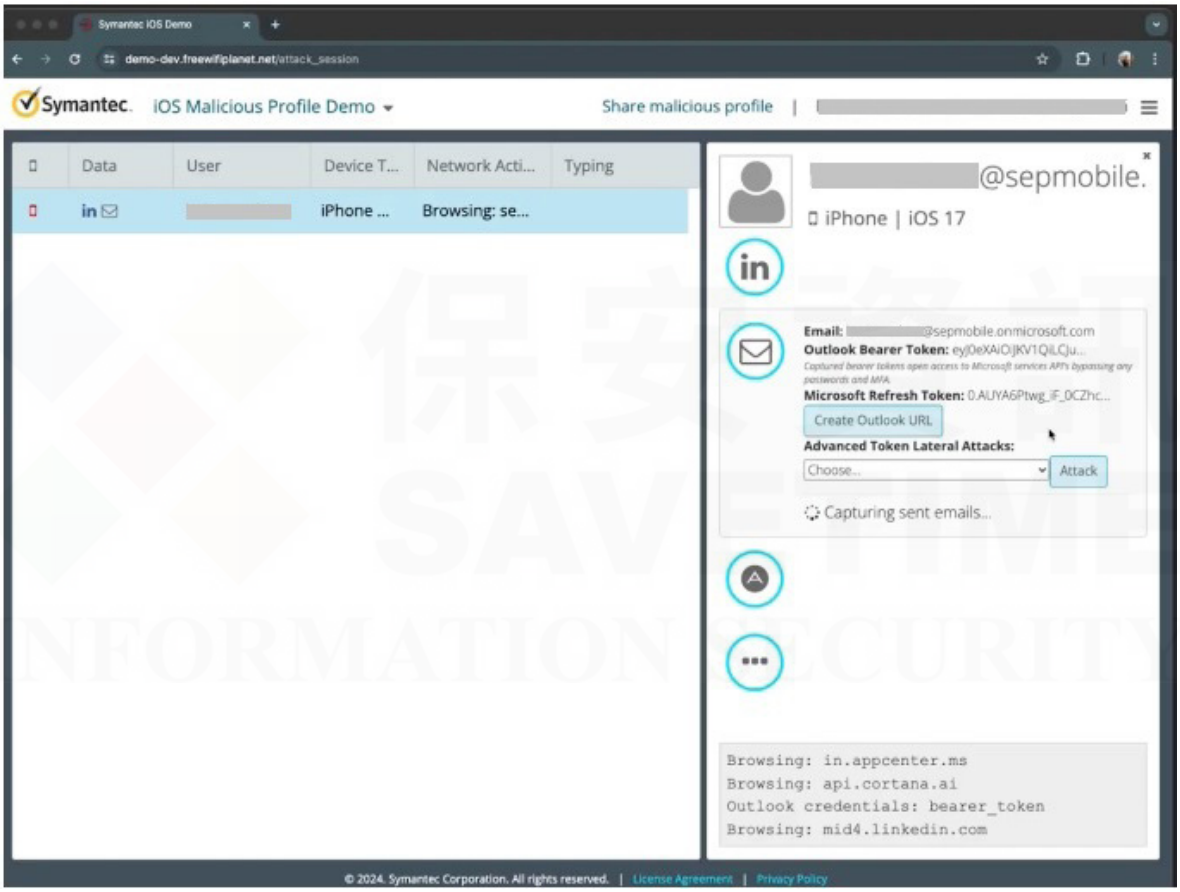
防護亮點：補足EMM不足，賽門鐵克行動威脅防禦(MTD)有效保護Microsoft身分識別平台內的識別碼權杖實例

當今的組織通常依賴一套被稱為企業行動管理解決方案 (Enterprise Mobility Management，EMM) 的政策與程序來監控與管理企業與員工的行動裝置。賽門鐵克最近檢視一家現實世界財富 500 大企業的行動裝置相關聯事件，該企業在全球擁有超過 400,000 名員工。我們團隊研究那些原本僅依賴 EMM 面對威脅的不堪一擊，與賽門鐵克行動威脅防禦 (MTD：Symantec Mobile Threat Defense) 保護所阻止攻擊形成的強烈對比。

拆解攻擊與解析 MTD 的防禦能力

其中一個攻擊媒介是利用惡意的 iOS 設定檔，透過中間人 (MiTM) 攻擊攔截 Microsoft 身分識別平台內的識別碼權杖。攻擊者以公司的 Active Directory 為目標，目的是繞過多因素驗證 (MFA) 來取得這些權杖--實際上就是存取公司資源的「通行天國之鑰」。

威脅者從公開和／或暗網收集員工聯絡資訊後，先發送大量的網路釣魚簡訊，偽裝成 IT 更新的訊息。當點選這些訊息時，就會下載惡意設定檔並安裝到員工的 iOS 裝置上。這些設定檔會重新路由和解密加密流量，讓攻擊者攔截敏感資料和存取公司資源 (例如：Outlook 和 Intune) 所需的憑證權限。



攻擊者如何存取使用者 Outlook 帳戶的範例

攻擊者濫用盜取的權杖，在網路中進行橫向移動，取得不受限制的存取權限，卻沒有觸發任何記錄或警示。所幸有使用賽門鐵克行動威脅防禦 (MTD：Symantec Mobile Threat Defense)，在端點識別並阻 止了這個攻擊鏈。

總而言之

- 該財富 500 大企業中有 3% 使用者成為簡訊網路釣魚攻擊的目標，所幸受到 MTD 提供的安全保護。
- 400 位使用者安裝不受信任的設定檔，因為有 MDM 保護，所以無法存取公司內部服務和資料。
- 25% 使用者成為採用解密用戶端流量的中間人 (MiTM) 攻擊之潛在目標。賽門鐵克 MTD 在攻擊者有機會存取公司內部服務和資料之前，就已識別並阻擋這些潛在攻擊。

如需關於行動平台上的攻擊和防護策略的更多深入見解，請參閱我們的白皮書《保護您的行動企業》：僅有 EMM 是不夠。

賽門鐵克的端點安全企業版 (SESE)／端點安全完整版(SESC)內含防護 IOS／Android 的最先進防護技術，請點擊此處瀏覽更完整的資訊。

2024/11/19

借力新版的LODEINFO後門，Earth Kasha駭客組織已開疆闢土至日本、台灣和印度

Earth Kasha 駭客組織採用不同的戰術、技術、流程 (TTPs)，透過部署各種後門惡意軟體 (例如：LODEINFO、NOOPDOOR、Cobalt Strike) 來開疆闢土至日本、台灣和印度的目標，同時專注於與先進科技和政府機構相關的單位。Earth Kasha 攻擊行動使用魚叉式網路釣魚或開採濫用已公開應用程式中的漏洞來嘗試初始存取。LODEINFO 後門一直是他們首選的後門，多年來一直不斷更新。最新 LODEINFO 後門支援多個後門指令，並與之前版本有所不同。最新版的 LODEINFO 也直接支援在記憶體中執行 DLL 或 shellcode，而不處理後門指令。它的整體能力包括執行任意 shellcode、截圖，以及將資訊滲出傳回攻擊者所操控的伺服主機。

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：

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.Gen.MBT
- WS.Malware.1

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。

2024/11/18

越來越多釣魚電子郵件的附件偏愛SVG影像格式，捨JPG／PNG等傳統影像

研究人員最近發現到有越來越多網路釣魚行動使用 SVG(Scalable Vector Graphics，可縮放向量圖形) 附件來發動網路釣魚和惡意軟體攻擊，以逃避偵測。與 JPG 或 PNG 等傳統影像格式不同，SVG 使用數學演算法來顯示影像，然後您可以將其縮放成任何大小，而不會對其品質造成負面影響。使它們成為瀏覽器應用程式的理想選擇，並且在惡意使用時較難偵測。

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。

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.Svg!gen2
- Web.Reputation.1
- WS.SecurityRisk.4

2024/11/18

GuLoader惡意軟體下載器所涉入的惡意垃圾郵件散播行動，最終會傳遞Remcos遠端存取木馬程式(RAT)

賽門鐵克的安全機制應變中心 (Symantec Security Response) 發現一起由 GuLoader 惡意軟體下載器所涉入的惡意垃圾郵件散播行動，該行動試圖傳送 Remcos 遠端存取木馬程式 (RAT) 的有效酬載。此惡意電子郵件行動首次出現於 11 月 18 日，利用 7zip 壓縮檔附件傳送包含一個惡意的 GuLoader vbs 檔案。一旦執行，惡意腳本會直接將 Remcos 有效酬載下載到記憶體中。然後 Remcos 會透過程序注入的方式啟動。

電子郵件主旨：Demand On Delivery - Track Shipment(*貨到付款 - 追蹤貨件動態)
電子郵件附件：DHL_Shipping_Invoices_Awb_BL_00000000011182024224782002003180817 4Global180030011182024.7z

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：

- Scr.Guloader!gen3
- Scr.Malcode!gen43
- VBS.Downloader.Trojan

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。

2024/11/18
使用Flutter框架開發的木馬化應用程式鎖定MacOS系統

在真實網路情境裡發現在 macOS 平台上有越來越多的機器感染全新惡意軟體。這些惡意軟體是利用 Flutter 架構所開發，Flutter 是一個用於設計跨平台應用程式的開放原始碼開發套件。已發現的惡意軟體檔案大多使用以加密貨幣為主題的名稱，在某些情況下可能會同時執行一些功能完整的應用程式或遊戲 (例如：Notepad 或 Minesweeper)。除了 Flutter 建立的惡意軟體之外，還發現採用 Golang 和 Python 語言所開發類似被植入木馬的應用程式。

網路上的知識：Flutter 是由 Google 開發和支援的開放原始碼架構。前端和完整堆疊開發人員使用 Flutter 為具有單一程式碼基底的多個平台建置應用程式之使用者界面 (UI)。

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
- 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。

2024/11/18
在Water Barghest惡意行動中亂竄的Ngioweb惡意軟體

根據趨勢科技最近一份報告，Ngioweb 惡意軟體最新後繼新變種已在被稱為「Water Barghest」正在進行中的惡意行動中亂竄。此行動利用易受攻擊的 IoT 裝置來傳送 Ngioweb 惡意軟體，並將受攻擊的裝置註冊為代理伺服器。攻擊者之後會透過 residential proxy 市集網站出售新納入的殭屍電腦。據估計，截至 2024 年 10 月，Water Barghest 行動已操控超過 20k 台受攻擊的 IoT (物聯網) 裝置。

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。

2024/11/18

在真實網路情境裡發現全新惡意竊密程式：PXA Stealer

PXA Stealer 是 Cisco Talos 研究人員發現的全新惡意竊密程式。此惡意軟體最近頻頻出現在歐洲和亞洲的政府單位和教育機構。PXA Stealer 標是收集和滲出各種敏感資料，包括憑證、一鍵自動填入的資料、加密貨幣錢包、銀行資訊、cookies、Discord 權杖或來自第三方應用程式 (例如：密碼管理器或 VPN 客戶端) 的資料等。

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-RgPst!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：

- Scr.Heuristic!gen20
- 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!400
- Heur.AdvML.A!500
- 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: 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。

2024/11/17
利用DLL側載技術來傳播的XLoader惡意軟體

研究人員發現一種名為 XLoader 的惡意軟體，此惡意軟體透過 DLL 側載進行傳播。在這種攻擊方法中，合法應用程式會與兩個惡意 DLL 檔案 (jli.dll 和 concrt140e.dll) 綁定在壓縮檔案中。當執行合法應用程式時，會在不知情的情況下載入並執行惡意 DLL，隨後觸發惡意軟體。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- WS.Malware.1
- W32.Silly!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。

2024/11/17
Melofee後門程式最新變種，鎖定RHEL 7.9作業系統

本月初，研究人員發現針對 Red Hat Enterprise Linux (RHEL) 7.9 作業系統的 Melofee 最新變種。該惡意軟體被認為與 Winnti 進階持續威脅 (APT) 駭客集團有所關聯。

Winnti 是知名的進階持續威脅 (APT) 駭客集團，主要從事網路間諜及財務行動。該駭客集團至少從 2009 年就嶄露頭角，經常涉入針對全球組織的惡意行動。該駭客集團常化名為 APT41、BARIUM 和 Wicked Panda 等，突顯其曾發動許多不同的攻擊行動。

根據報告，此 Melofee 變種的重要更新包括 RC4 加密的核心驅動程式，可隱藏檔案、程序和網路連線。此外，該惡意軟體還加強持久性機制，並改善識別目標的功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- 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。

2024/11/15

BabbleLoader採用垃圾程式碼插入技術，讓安全軟體措手不及

駭客圈使用諸如「BabbleLoader」等惡意程式載入器由來已久。BabbleLoader 採取迴避措施，以防範許多形式的偵測。此惡意程式載入器主要特徵包括大量的垃圾程式碼插入來改變形態與特徵，這會改變載入程式的結構和流程，有效地避開基於簽章、人工智慧和行為偵測等安全偵測技術。針對講英語和俄語的人進行各種宣傳活動，引誘他們下載例如：影片編輯、遊戲、VPN、瀏覽器和工具程式的破解版。其他攻擊行動目標是財務和管理方面的企業專業人員，偽裝成會計軟體，以及人力資源或薪酬管理專業人員常用的填寫資格審核表格。

網路上的知識：垃圾程式碼是一種技術，用於向程式中添加無意義或不相關的指令，以使反組譯工具更難準確解釋程式的行為。這種技術通常被惡意軟體作者使用，以使分析人員更難逆向工程惡意軟體並理解其行為。

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

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.Gen.9
- W32.Silly!gen
- WS.Malware.1
- WS.Reputation.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.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C
- Heur.AdvML.S.N
- Heur.AdvML.SN.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。

2024/11/15

WezRAT遠端存取木馬(RAT)惡意軟體

WezRAT 是一種基於 C++ 的模組化惡意軟體，屬於知名的 Emennet Pasargad 威脅組織所有。根據 Checkpoint 發佈最新報告，WezRAT 已經出現在近期針對以色列多個組織的攻擊行動中。此惡意軟體具有多種功能，例如：執行任意指令、鍵盤側錄、收集遭入侵系統的資料、下載任意檔案、竊取剪貼簿或 cookies 等。擷取之資訊會傳送到攻擊者控制的 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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- 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：

- Trojan Horse
- 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
- 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。

2024/11/15
以macOS平台為目標的全新特洛伊木馬程式：RustyAttr

RustyAttr 是以 macOS 平台為目標的全新特洛伊木馬程式。該惡意軟體被認定為 Appleworm 進階持續威脅 (APT) 駭客集團 (也稱為 Lazarus) 所為，根據多項網路指標顯示，該惡意軟體的最新散佈行動與該駭客集團先前發動的攻擊有關，可信度中等。RustyAttr 是採用桌面應用程式開發工具--Tauri 開發的，Tauri 是用於建立桌面和行動 APP 的開放原始碼框架。該惡意軟體透過擴展檔案屬性，利用新的程式碼偷運 (code smuggling) 技術，試圖逃避偵測。觀察到的惡意軟體樣本一開始就帶有遭洩露的憑證簽章，但該憑證後來被蘋果公司撤銷。

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
- 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。

2024/11/15
HawkEye惡意竊密程式

HawkEye 惡意軟體 (也稱為 Predator Pain) 是一個老牌的惡意軟體家族，在威脅生態圈已活躍超過 14 年。最初是以鍵盤側錄器打響名號，後來進化成更完整的惡意竊密程式，經常出現在其他惡意軟體家族涉入的攻擊行動中。通常觀察到的散佈方式可能包括魚叉式網路釣魚郵件或惡意廣告等。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

- SONAR.Infostealer!g3
- SONAR.Stealer!gen2
- SONAR.SuspBeh.C!gen18
- SONAR.SuspLaunch!g22
- 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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Packed.31
- Packed.Generic.496
- PasswordRevealer
- Scr.Malcode!gdn30
- Scr.Malcode!gdn34
- Trojan.Gen
- Trojan.Gen.2
- Trojan.Gen.MBT
- 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

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。

2024/11/14

利用ClickFix的社交工程伎倆傳播Glove Stealer惡意竊密程式

Glove Stealer 是在 .NET 開發者平台開發的惡意竊密程式，透過偽裝成疑難排解工具的釣魚電子郵件散佈，使用類似 ClickFix 的社交工程伎倆來欺騙使用者。它以各種瀏覽器、加密貨幣錢包、密碼管理器、電子郵件用戶端和其他本機安裝軟體的敏感資料為目標，利用 IElevator 服務繞過加密，從瀏覽器擴充套件和應用程式竊取資訊。

網路上的知識：ClickFix 社交工程伎倆，泛指藉由偽造錯誤訊息視窗 (例如：佯稱麥克風或是耳機出現異常)，引誘使用者按下 Fix it 或 Try Fix，使用者若是依照指示操作，對方就會在這個時候安裝惡意程式。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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。

2024/11/14

天下沒有白吃的午餐～破解版軟體免費奉送惡意竊密程式：Steelfox

安全研究人員報告一種名為 Steelfox 的特洛伊木馬程式在真實網路情境裡傳出災情。此木馬程式主要透過部落格及論壇文章散播包括 Foxit PDF 閱讀器、JetBrains 及 AutoCAD 等熱門軟體的破解版的廣告。如果用戶被誘騙下載該檔案，一經執行就會安裝這個能滲出資料與挖礦綁架的惡意竊密程式。

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.SuspDriver!gen5
- SONAR.SuspDriver!gen6
- SONAR.SuspDriver!gen10
- SONAR.SuspDriver!gen11
- SONAR.SuspDriver!gen1
- SONAR.SuspDriver!gen2
- SONAR.Trafic2.RGC!g10

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.Dropper

- Trojan Horse
- WS.Malware.2

基於機器學習的防禦技術：

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

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**。