保安資訊--本周(台灣時間2024/11/15)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 7,100 台受保護端點上總共阻止了 4,460 萬次攻擊。這些攻擊中有 78.2% 在感染階段前就被有效阻止：**(2024/11/11)**

- 在**8萬4,300**台端點上，阻止了**1,230**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬8,400**台端點上，阻止了**800**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬7,900**台**Windows**伺服主機上，阻止了**6萬9,000**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**1萬400**台端點上，阻止了**70萬7,600**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,800**台端點上，阻止了**240**萬次嘗試利用的應用程式漏洞。
- 在**12萬7,700**台端點上，阻止了**250**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**6,200**台端點上，阻止了**97萬5,900**次加密貨幣挖礦攻擊。
- 在**10萬1,400**台端點上，阻止了**880**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**472**台端點上，阻止了**8萬9,900**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 5,300 個受保護端點上阻止了總計 810 萬次攻擊。**(2024/11/11)**

- 使用網頁信譽情資，在 **186.3K** 個端點上阻止 **760** 萬次攻擊。
- 攔截 **21.7K** 個端點上 **285.4K** 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 **8.6K** 個端點上攔截 **188K** 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 **488** 個端點上攔截 **10.1K** 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。

2024/11/14

與哈馬斯有關聯的WIRTE駭客集團繼續以不斷演變之策略發動網路攻擊行動

Check Point Research 報導與哈馬斯有關聯的駭客集團：WIRTE 所發動的網路攻擊行動，該行動專門針對中東國家的機構組織，利用區域事件進行攻擊。該行動使用 IronWind 惡意軟體載入器，可進行與指揮與控制 (C&C) 伺服器的通訊，並執行隱藏在 HTML 語法中的惡意程式碼。雖然該組織的工具已有所演變，但其核心策略仍保持一致，包括使用特定網域命名慣例、透過 HTML 標籤進行通訊、限制使用者代理程式回應，以及重導向至合法網站。

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.Ransom!gen14

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.Gen.MBT
- Trojan Horse
- 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。

2024/11/14

新出現的銀行惡意軟體：Silver Shifting Yak

Silver Shifting Yak 是 SciLabs 研究人員發現一種新的 C++ 型銀行惡意軟體。此惡意軟體的目標是滲透超過 50 家金融機構的銀行資料，例如：Banco Itaú、Banco do Brasil、Banco Bandresco、Foxbit、Mercado Pago Brasil 等。Silver Shifting Yak 也可能嘗試竊取各種微軟入口網站使用的憑證，包括 Azure、Outlook 和 Xbox。此惡意軟體的初始攻擊階段被認為是由網路釣魚行動所觸發，這些行動會將受害者導向代管在偽造網站上的惡意 .zip 壓縮檔。

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：

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!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：

- 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。

2024/11/13

又見好工具濫用成為凶器：濫用Chisel 和Netskope工具發動精密的 PowerShell 網路攻擊行動

有人發現一個複雜的多階段 PowerShell 攻擊行動，利用 LNK 捷徑檔案觸發一系列混淆腳本，導致惡意有效酬載的下載和執行。該攻擊涉及三個階段的 PowerShell 指令碼，以建立持久性、與 C&C 伺服器通訊，並執行接收到的指令。此攻擊行動使用 Chisel 進行快速 TCP／UDP 通道，並使用 Netskope proxy在受攻擊的網路內進行橫向移動。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Ps-RgPst!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
- Web.Reputation.1
- 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。

2024/11/13

散播Formbook惡意竊密程式的網路攻擊行動正在肆虐義大利用戶

研究人員最近發現一起以義大利用戶為目標的惡意垃圾郵件攻擊行動，散佈以竊取資訊能力著稱的 Formbook 惡意竊密程式。該行動利用一封以催繳單為幌子的電子郵件，製造收件人打開隨附的 7Z 壓縮檔案緊迫感。如果受害者打開檔案並執行惡意軟體的有效籌負，就會啟動惡意軟體的資訊竊取的序曲。

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.Formbook
- Trojan.Gen.MBT

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

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。

2024/11/13

舊瓶裝新酒～LodaRAT惡意軟體以新功能颳起新旋風

LodaRAT 是早在 2016 年就被發現的老牌遠端存取木馬 (RAT)，最近在持續的惡意垃圾郵件散播行動中再度被發現，其新功能是可以從 Microsoft Edge 和 Brave 竊取 cookies 和密碼。此惡意軟體以 AutoIt 寫成，原本透過網路釣魚傳播，但現在使用 DonutLoader 和 Cobalt Strike。它偽裝成 Discord、Skype 和 Windows Update 等軟體，功能包括資料外洩、傳遞其他惡意軟體、螢幕擷取，以及控制受害者的鏡頭和滑鼠。

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-Schtsk!g1
- ACM.Ps-Wscr!g1
- 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：

- Trojan.Gen.MBT

- 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。

2024/11/13

進階持續性威脅(APT)駭客組織：TAG-112，在西藏網站使用惡意JavaScript部署Cobalt Strike

據報導，與中國有關聯的進階持續性威脅 (APT) 駭客組織：TAG-112 發起一場網路攻擊行動，他們入侵西藏的網站來部署 Cobalt Strike 惡意軟體。威脅者在網站上嵌入惡意 JavaScript，偽造 TLS 證書錯誤，誘騙瀏覽者下載偽裝的安全憑證。此惡意軟體最終在執行時會載入 Cobalt Strike 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

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

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。

2024/11/12

Arcus Media～採用「雙重勒索」策略打響名號的勒索軟體集團

Arcus Media 是一個以採用「雙重勒索」策略打響名號的勒索軟體集團。所謂「雙重勒索」策略就是除了加密檔案外，攻擊者還會竊取受害者的敏感資料，並威脅如果受害者不支付贖金，這些資料將被公開或賣給第三方。這樣的方式大大增加受害者支付贖金的壓力，因為公開洩漏敏感資料可能會對企業的商譽、法律責任及客戶隱私造成嚴重的影響，也因此讓勒索軟體攻擊的成功率和贖金金額顯著上升。Arcus Media 勒索軟體透過網路釣魚和漏洞開採濫用以取得初始存取權，並開採濫用遠端桌面協定 (RDP) 漏洞和就地取材技倆行橫向移動。近幾個月來，其惡意程式已在政府、銀行業、建築業、IT 服務業及娛樂業等多個行業造成多位受害者。

被加密的檔案會冠上 [encrypted].arcus 的副檔名。勒索贖金支付說明文字檔 (Arcus-ReadMe.txt) 會被放置在多個位置，並透過威脅和明確的指示，迫使受害者迅速就範。開啟贖金說明時，它會通知受害者所有敏感資料已被加密並已外流，這意味著雙重威脅：資料不僅無法存取，還會落入攻擊者手中。

攻擊者會指示受害者透過安全且匿名的 Tox 聊天工具與他們聯絡，並提供特定的 ID 用於傳送訊息，以及備用的電子郵件地址，以防他們在 24 小時內沒有回覆。他們建立明確的事態升級時間表：如果受害者在三天內沒有聯繫，他們就威脅要在他們「洩漏網站」上公開竊取的資料，並警告洩露資料可能會嚴重損害組織的信譽，並導致違反 GDPR 法規遵循問題。

網路上的知識：Tox是一個使用端到端加密及對等網路的即時通訊和影片電話協定，遵循 GNU 通用公眾授權條款協定釋出。該專案的目標是為所有人提供安全而方便的通訊方式。Tox 使用者將會分配到一個公鑰和一個私鑰，之後直接通過一個分散式對等網路互相連接。使用者可以通過 Tox 給朋友傳送資訊、語音或進行影片聊天，群聊或傳送檔案。所有通過 Tox 的流量將使用 NaCl 進行端到端加密。

五天後若沒有聯絡，攻擊者表示所有已取得的資料--包括敏感的客戶資訊、財務細節和合約--都會被完整地公開。他們還進一步說明，建議受害者不要嘗試修改加密檔案或停止加密程序，因為任何一個動作都可能導致永久性的資料遺失。

Arcus Media 勒索軟體集團透過結合期限壓力、企業的商譽、法律責任及客戶隱私造成嚴重的影響，目的在於最大化受害者的心理壓力，使其迅速乖乖就範。

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.Wmic-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g195
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g21

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

基於機器學習的防禦技術：

- Heur.AdvML.A!500

2024/11/12

防護亮點：賽門鐵克有效應對， 以TGZ附件來陳倉暗度GuLoader惡意軟體下載器的電子郵件攻擊

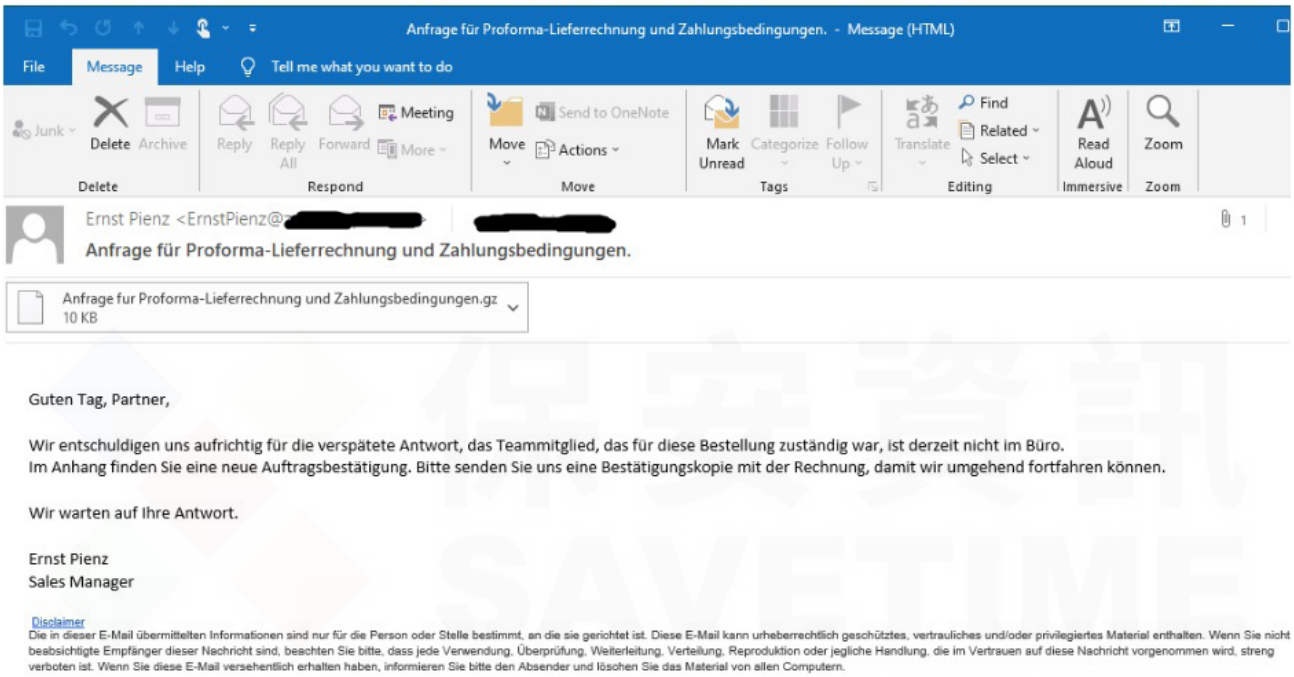
GuLoader 也稱為 GuLoad，是一種知名的惡意軟體下載器，自 2019 年出現以來一直困擾著電腦系統的資安威脅。多年來，此惡意軟體經過多年的開發和測試已經展現重大的轉變，可以根據最新的情況不斷調整適應以逃避偵測並利用新的漏洞。

最近幾週，我們在遙測資料中觀察到與 GuLoader 的電子郵件有關的流量變明顯，每天偵測到的數量高達數百封。這些電子郵件通常在本文中包含一則訊息，目的是引誘收件者打開附件並執行其中檔案。值得注意的是，.GZ 附件檔案名稱比之前執行的 GuLoader 更長，範例包括：

- Anfrage fur Proforma-Lieferrechnung und Zahlungsbedingungen.gz
- Aqua & Clean LTD - Order Inquiry,Pricing and Shipping Costs - 11524.gz
- Draft_Shipping_documents_0020331110111.gz
- Advice Copy-$72,000-114571_pdf.gz
- Anfrage fur Proforma-Lieferrechn
- Anmodning om levering af proformafaktura og betalingstilstand.gz
- Baratti & Milano S.R.L Cooperation 10_24_2024.gz
- CR-FEDEX_TN-779454699153_DT-MRN_CD-20241023_CT-1934.gz
- Draft_Shipping_documents_0020331110111.gz
- EuroStar Machinery -14240 - PPD 221-29-10-2024.gz
- Kemilab - 291024 Updated price list.gz
- PO 25367 for Seacole - ORD ACK 216668.gz
- Upit W.D. Concord West d.o.o. nr.10072024.gz
- oferta urgente CAF Mexico NCR NCR 6927 09022024.gz
- DHL Documentos De Envo 0020331110114.gz
- DHL Shipping DOC_BG468545215485_pdf.gz
- Dringende Bestellung 10_24_2024.gz
- Hitna ponuda LUKINTEHNIK, d.o.o. 10242024.gz
- NUEVO_ORDEN_DE_COMPRA_3010202400012709.gz

- Odhad IMP3816 pro vyvoz v poslednim ctvrtleti.gz
- PO 25367 for Seacole - ORD ACK 216668.gz
- SBR & Co-14240 - PPD 221-29-10-2024.gz
- Stima IMP87654 per l'esportazione dell'ultimo trimestre.gz
- Urgent ORDER -Nesma And Partners - SICIM JV.gz

這些電子郵件使用社交工程技倆引誘使用者開啟附件。這些技術包括待處理的包裹、不存在的訂單更新，或因尚未收到貨款而寄倉的訂單。



這些老套的社交工程技倆已經流行好多年了，但不知情的使用者仍會上當。隨著年終假期即將來臨，我們預期這些手法會增加，因為網路購物已經增加。

攻擊者可能選擇 TGZ／GZIP 這種較不常見的壓縮檔案格式，以降低被安全軟體偵測到的風險。TGZ／GZIP 格式也提供較佳的壓縮效果，讓附件檔可以更小。

在 .GZ 附件中，有一個與 .GZ 本身名稱相同的惡意 .VBS 檔案。

在這起 GuLoader 攻擊中，我們觀察到壓縮檔內的 VBS 檔案有各種版本，使用多種技術來逃避模擬並隱藏程式碼的意圖，同時在檔案中填入大量註解，試圖使其看起來合法。

```
'Perlekrans. tibbit thirdborough. infract
'Beechy, hvdvundne. distn majli oxozonides
'Subcommissary genindlser: prohibitorily templarlikeness tintinnabulation.
'Vitrify, udlbet. programmingen pulvillar rapped50
'Alarum! firebird; brsuro; reclusory rupture91
'Blikfang. stationerer.
'Snitgrnt, fender, modgift. tractarian
'Ciliform bedaarelsen. underprikningens, sodomittens nordom106;
'Pennes. mitigatory
'Okkuperet! pasningerne ununiformness diphenan,
'Intrafistular elbilerne
'Annats, pleiophyllous lemurinae;
'muffishness! kommandolinjerne
'Regionplanlgningens, departer rekordmassakre?
'Ephorus teaktrsstols: tellurite,
'Prkener; gopler! sedges mbelpolituren tenderised!
Set Technicalizes = Vanrys.ExecQuery("Select * from HNet_ConnectionProperties")
'Romantiseringers59 traumatiseret sicarious. linns?
'Ccilias; skuespillerprstationers; benshi.
'busaos: bevbnendes! nonobservingly. fewtrils
'Forraadnelsesprocesserne, indbetalingskortets: printeradresser68. similis
'Sife? ordeals uranic: kinin;
'Ankomsthallerne: menneskeliggrelsernes; commissar ubestridte? teleudstyrets;
'Alvild? bderegn? periodicitets. brnetestamenterne afkogningen.
'Tursio; udkonkurrerede;
'Balibago gumminess surres11. levnedsmiddelkontrollernes skotlands
```

也經常可以看到非常多的變數自我串接。

```
Paraesthetic = Paraesthetic & "hiswordle g"
Paraesthetic = Paraesthetic & "odsejeres Sawor"
Paraesthetic = Paraesthetic & "dsarbejd"
Paraesthetic = Paraesthetic & "erne Slyngerne Hurwor"

Subareoletfragtgod = Trim("Mongolsk")

Paraesthetic = Paraesthetic & "digbussers "
Paraesthetic = Paraesthetic & "Kalvekrsewords Sciroc"
Paraesthetic = Paraesthetic & "coer #>"
Paraesthetic = Paraesthetic & ";$Cranio"
Paraesthetic = Paraesthetic & "logisworda"
Paraesthetic = Paraesthetic & "gwordwordagelses"
Paraesthetic = Paraesthetic & "evnens='Acha"
Paraesthetic = Paraesthetic & "fe';<#Hensynsfu"
Paraesthetic = Paraesthetic & "ldheder"
Paraesthetic = Paraesthetic & "ne wordxword . c"
Paraesthetic = Paraesthetic & "nysenes Overreligious Un"
Paraesthetic = Paraesthetic & "derindekseword o"
Paraesthetic = Paraesthetic & "wordosclero"
Paraesthetic = Paraesthetic & "sis #>;$Skarksen="
Paraesthetic = Paraesthetic & "$hosword.PrivawordeDa"
Paraesthetic = Paraesthetic & "worda;If ($Skarksen"

Mrkedesfacetteresc = Left("Aabenbaring125",220) & "Revictualled"

Paraesthetic = Paraesthetic & ") {$De"
Paraesthetic = Paraesthetic & "kanworderedes++;}"
Paraesthetic = Paraesthetic & "funcwordion "
Paraesthetic = Paraesthetic & "glewordsjerskred"
Paraesthetic = Paraesthetic & "($wor"
```

在 VBS 檔案中使用大型循環可以用來迴避，例如：讓一個陣列被指定給一個變數超過 387 萬次的重複。

```
    for Skrubnings34=0 to 3874241
    Usikkerhederne= array(65+5+0,69,77,59,72,73,62,59,66,66)
    Next
```

在其他情況下，會使用字串操作來建立下一步，也就是 PowerShell 指令。

```
Djvlehovederes = Djvlehovederes + Fllesnavnets & Aktivator & "he" + Lwp + Lwp

Djvlehovederes = Djvlehovederes + "." + "e" & "x" & "e"
```

```
Centrumdemokraternes = Centrumdemokraternes & "<#Calc32altary Direktrpost
Centrumdemokraternes = Centrumdemokraternes & "ity';$Erkendt='\Legetjsforr
Centrumdemokraternes = Centrumdemokraternes & "Kar) in ';$Rehide=$Overveje
Centrumdemokraternes = Centrumdemokraternes & "rmHartxtAmbTDefeDtxtaX luTh


Set Sternsons = CreateObject("Shell.Application")
```

```
Centrumdemokraternes = Replace(Centrumdemokraternes,"Calc32",Aktivator)
```

```
Centrumdemokraternes = Replace(Centrumdemokraternes,"txt",".")
```

```
Call Sternsons.ShellExecute(Djvlehovederes, Chr(34) & Centrumdemokraternes & Chr(34), "", "",
```

賽門鐵克的防護技術涵蓋多個層級，包括在電子郵件傳送的初始階段封鎖攻擊。此外，還採取行為和適應性防護 (Adaptive Protection) 措施。為了提供強大的涵蓋範圍，以檔案為基礎的偵測也涵蓋惡意 VBS 檔案。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g111

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!gen*
- ISB.Heuristic!gen*

- Scr.Heuristic!gen*
- Trojan Horse
- Web.Reputation.1

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。
要了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解 Symantec Endpoint Security 的 Adaptive Protection，請點擊此處。
欲深入瞭解更多有關賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，請點擊此處。

2024/11/12

CVE-2024-5910存在Palo Alto Network遷移和組態管理工具：Expedition的身分驗證漏洞

CVE-2024-5910 是存在 Palo Alto Network 的移轉工具 Expedition 嚴重等級 (CVSS 風險評分：9.8) 身分驗證漏洞，Expedition 是管理員廣泛使用的防火牆遷移和組態管理工具。成功開採濫用此漏洞可讓具有網路存取權限的攻擊者利用此漏洞接管管理員帳戶，並可能存取敏感的組態機密、憑證和儲存在工具中的其他資料。此問題影響 Expedition 1.2.92 以前的版本。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。

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: Palo Alto Missing Authentication CVE-2024-5910

2024/11/11

最近正在發送Rhadamanthys惡意竊密程式的魚叉式網路釣魚行動

Rhadamanthys 惡意竊密程式的最新變種，被發現正在透過魚叉式網路釣魚攻擊傳送，目標是北美 (NAM)、拉丁美洲 (LAM)、歐洲 (EU)、中東 (ME) 和亞太地區及日本 (APJ) 的使用者。這起新行動主要是透過免費網路電子郵件服務傳送，並聲稱與侵犯版權有關。寄件者包含一個網址鏈結，指向版權資料的「移除指示」，但實際上這些鏈結會指向包含 Rhadamanthys 的公共檔案分享網站所託管的密碼保護檔案。這些受密碼保護的檔案通常包含 3 個檔案，一個用於側載 DLL 的合法可執行檔案、一個 DLL 形式的 Rhadamanthys 惡意竊密程式，以及一個誘餌 ESPS 或 PDF 檔案。這個最新變種還增加一些額外的功能，例如：光學辨識 (OCR)，用於掃描目標機器上的文件以獲取加密錢包密碼。

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-Reg!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.6
- Trojan.Gen.MBT
- WS.Malware.1
- 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!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。

2024/11/11

Remcos遠端存取木馬(RAT)在出現在最近網路攻擊行動

Fortinet 的 FortiGuard 實驗室研究人員報告一個散佈 Remcos 遠端存取木馬 (RAT) 的全新網路攻擊行動。攻擊者利用含有惡意 MS Excel 附件的釣魚電子郵件。此行動嘗試濫用 Microsoft Office CVE-2017-0199 的舊漏洞。一旦成功開採濫用此漏洞，惡意 .HTA 檔案就會被植入受感染的機器上。攻擊鏈的進一步階段涉及執行多個腳本和 PowerShell 指令，最後導致 Remcos RAT 傳送至受害者。這個版本的 Remcos 具有多種功能，包括從受感染的端點收集資料、執行 shell、修改登錄機碼、服務和程序管理、下載／執行額外的任意二進位檔案等。

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.Untrst-RunSys!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。

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!gen12
- ISB.Downloader!gen80
- Scr.Malcode!gen59
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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：

- Attack: Malicious RTF File CVE-2017-0199
- System Infected: Trojan.Backdoor Activity 757
- 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。

2024/11/11

針對macOS使用者的「Hidden Risk*隱藏風險」網路攻擊行動

據報導，一起全新的網路惡意行動針對 macOS 使用者，稱為「Hidden Risk*隱藏風險」。此行動是由被稱為 BlueNoroff 的駭客組織所為。該行動利用與加密相關新聞和趨勢的各種誘惑。遭感染後，使用者會收到一份關於特定加密貨幣主題的誘餌 .pdf 文件檔，同時在背景中下載惡意二進位檔，並在受害者的機器上執行。攻擊者的戰術、技巧和程序 (TTPs)、部署的有效酬載和使用的網路基礎架構都與 BlueNoroff 駭客組織過去的攻擊行動有某些相似之處。

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：

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。

2024/11/11

利用WordPress之Calendar Event Multi View WordPress 外掛存在的 Cross-Site Scripting(XSS)跨站攻擊 (CVE-2021-24498)嘗試增加

CVE-2021-24498 是存在 WordPress 之 Calendar Event Multi View 外掛程式中的 Cross-Site Scripting(XSS) 跨站攻擊漏洞，此外掛程式設計是透過建立不同檢視的行事曆來管理事件。成功開採濫用此漏洞可讓攻擊者將惡意指令碼注入受影響的網站，導致存取敏感資料，例如：登入認證和付款資訊等。此問題會影響 1.4.01 之前的外掛程式版本。賽門鐵克的網路層防護技術：入侵防護系統 (IPS) 已根據威脅趨勢監控進行掃描，顯示最近利用此三年前漏洞的嘗試有所上升。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：

- Attack: Malicious RTF File CVE-2017-0199
- System Infected: Trojan.Backdoor Activity 757
- Web Attack: Webpulse Bad Reputation Domain Request

2024/11/10

Androxgh0st (Mozi)殭屍網路重出江湖

最近有報導指出 Mozi 殭屍網路重出江湖，目前以 Androxgh0st 的名義運作，至少從 2024 年 1 月開始就以物聯網裝置、Web 伺服器和其他平台為目標。Androxgh0st 的功能包括竊取憑證和濫用漏洞 (例如：PHPUnit 和 Apache 中的漏洞)，以及透過 Web shells 維持持久性／常駐能力。它利用 SMTP 來濫用暴露的憑證和 API，並針對 .env 檔案來取得敏感資料。這些能力允許它滲透網路並建立對受攻擊系統的控制，對基礎架構構成重大威脅。據研究人員指出，此行動背後的行動者正在開採濫用 CVE-2023-1389 和 CVE-2024-36401 等漏洞。

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

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: TP-Link Router Remote Code Execution Vulnerability CVE-2023-1389
- 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
- Web Attack: Malicious Shell Script Download 2

2024/11/10

Skuld和Blank Grabber透過惡意的npm套件傳播

最近的一次網路攻擊以 Roblox 開發人員為目標，散佈惡意的 npm 套件。研究人員指出，攻擊者利用類似而錯誤的名稱 (typosquatting) 來建立名稱與合法名稱相似的套件，例如：「node-dll」。一旦安裝，這些套件就會下載並執行稱為 Skuld 和 Blank Grabber 的惡意竊密程式。這些威脅能夠竊取敏感資訊，例如：密碼和其他機密資料，然後透過 Discord webhooks 或 Telegram 洩露給攻擊者。

網路上的知識：Node Package Manager 又稱為 npm，字面上的意思來看，就是一個管理 node 的工具，npm 提供開發者用來分享、發布和管理 Node.js modules 的平台和工具。

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.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Ps-Enc!g1
- ACM.Untrst-Csc!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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Malscript!gen9
- Trojan.Gen.MBT

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: PowerShell Process Accessing discordapp
- Audit: System Process Accessing discordapp

2024/11/08

得力於RingQ Loader惡意軟體的助力，Silent Skimmer網路威脅行動勢如破竹

根據 Palo Alto Unit42 研究人員發佈最新報告，RingQ Loader 惡意軟體已在最近被稱為 Silent Skimmer 的攻擊行動中被扮演要角。為了入侵目標網路，攻擊者開採濫用兩個較舊的 Telerik 框架漏洞 CVE-2017-11317 和 CVE-2019-18935。在受害者的環境中取得立足點後，攻擊者使用各種 webshell、反向代理工具、Godpotato 權限升級工具、Cobalt Strike 以及 RingQ Loader 惡意軟體。後者可用作反射式載入惡意二進位檔案，以及下載額外任意有效酬載。

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-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2

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!gm1
- Backdoor.Trojan
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- 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：

- Web Attack: Telerik UI Arbitrary File Upload CVE-2017-11317
- Web Attack: Telerik UI CVE-2019-18935
- Web Attack: Telerik UI CVE-2019-18935 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。

2024/11/08

Mr.Skeleton RAT--源於njRAT遠端存取木馬(RAT)程式碼的全新變種

Mr.Skeleton 遠端存取木馬 (RAT) 是在近期真實網路情境中發現到一支全新遠端存取特洛伊木馬 (RAT)。該 RAT 源於著名的 njRAT(也稱為 Ratenjay) 惡意程式家族的程式碼。最近，Mr.Skeleton 在暗網上進行廣告銷售。該 RAT 的功能包括遠端存取和桌面操作、竄改檔案／資料夾和登錄檔 (Registry)、遠端 shell 執行、鍵盤側錄以及遠端控制裝置的鏡頭。

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-FlPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.Ratenjay!gen1
- SONAR.Ratenjay!gen2
- 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。

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：

- Backdoor.Ratenjay
- Backdoor.Ratenjay!gen1
- Scr.Malcode!gdn14
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/11/08

G700--行動裝置平台出現Craxs遠端存取木馬(RAT)的新變種

G700 是源於於 Craxs 遠端存取木馬 (RAT) 的新變種。該惡意軟體會濫用 Android 權限，以存取受攻擊裝置上儲存的敏感資訊，包括簡訊、電話聯絡人、裝置位置和裝置上儲存的檔案。G700 還有針對竊取憑證和銀行資料、攔截一次性密碼 (OTP) 和操控加密貨幣交易等額外功能。據報導，這個新 Craxs 變種是透過各種地下論壇以及 Telegram 頻道散佈。

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.1
- Android.Reputation.2
- Spyware:MobileSpy

2024/11/08

發現被命名為「VEILDrive」的網路攻擊行動

研究人員發現一起名為「VEILDrive」的網路攻擊行動，自 2023 年起持續進行。此攻擊行動會利用 Microsoft 的雲端服務 (包括 Teams、SharePoint、Quick Assist 和 OneDrive) 來攻擊組織，據了解此行動來自俄羅斯。攻擊者利用這些平台傳送魚叉式釣魚電子郵件和儲存惡意檔案。與此行動相關惡意軟體是基於 Java 的 [.]jar 檔案，未受保護且容易讀取。然而，儘管它很簡單，此惡意軟體仍能躲過端點偵測與回應 (EDR) 等高階安全軟體的偵測。

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.Ps-Rd32!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- RemoteAccess.Gen

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。

2024/11/07

GodFather惡意軟體出現更隱匿的新變種

在針對 500 多個銀行和加密應用程式的攻擊行動，發現 GodFather 惡意軟體的後繼新變種。該攻擊已擴大到日本、希臘、新加坡和亞塞拜然等國家。一開始，釣魚網頁冒充澳洲政府的 MyGov 網站，散佈與 GodFather 相關聯的 Android 套件檔 (APK)。惡意軟體利用無障礙服務來竊取銀行憑證，可自動執行裝置動作，而且威脅者會追蹤訪客以計畫進一步攻擊。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

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

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。

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**。