保安資訊--本周(台灣時間2024/08/23)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 5,400 台受保護端點上總共阻止了 4,720 萬次攻擊。這些攻擊中有 81.5% 在感染階段前就被有效阻止：**(2024/08/19)**

- 在**8萬9,600**台端點上，阻止了**1,110**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**10萬9,700**台端點上，阻止了**900**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬1,600**台**Windows**伺服主機上，阻止了**76**萬次攻擊。
- 在**5萬3,200**台端點上，阻止了**160**萬次嘗試掃描伺服器漏洞。
- 在**9,800**台端點上，阻止了**57萬5,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,700**台端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在**14萬3,200**台端點上，阻止了**610**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,700**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**9萬5,100**台端點上，阻止了**780**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**569**台端點上，阻止了**7萬9,400**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 10 萬 6,800 個受保護端點上阻止了總計 300 萬次攻擊。**(2024/08/19)**

- 使用網頁信譽情資，在 **98.5K** 個端點上阻止 **260** 萬次攻擊。
- 攔截 **18K** 個端點上 **308.6K** 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 **6.8K** 個端點上攔截 **60.7K** 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 **182** 個端點上攔截 **5.2K** 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。

2024/08/22

NGate--安卓平台上會將NFC資料傳送給攻擊者的全新手機惡意程式

一起利用被稱為 NGate 全新安卓平台手機惡意軟體的攻擊行動，已針對捷克銀行的使用者。NGate 使用一種新穎的技術，將受害者支付卡中的 NFC(近場通訊) 資料經由受攻擊的安卓手機傳輸至攻擊者的裝置。攻擊者就可以在他們的設備上模擬被盜的卡，並用於提款操作。據報導，惡意軟體是透過偽裝成合法服務的各種網站散佈。NGate 攻擊者使用的網路架構顯示是舊式的網路釣魚活動，會散佈惡意漸進式網路應用程式 (PWA) 和 WebAPK 。

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。

- AdLibrary:Generisk
- 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。

2024/08/22

北韓駭客組織puNK濫用Windows捷徑檔傳播Lilith遠端存取木馬(RAT)

已偵測到一個先前未被識別的北韓威脅組織，其名稱為 puNK，使用 Windows 捷徑 (LNK) 檔案散佈惡意軟體。當執行時，這些 LNK 檔案會從攻擊者的伺服器下載 AutoIt 腳本，隨後擷取最後的有效酬載荷：Lilith RAT。Lilith RAT 以 C++ 寫成，是一款開源的遠端控制軟體，方便進行其他遠端操作。

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.Ps-Schtsk!g1
- ACM.Ps-SvcReg!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：

- CL.Downloader!gen20
- CL.Downloader!gen204
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.NPE
- WS.SecurityRisk.4

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。

2024/08/22

Insom勒索軟體

Insom 勒索軟體是 Makop 勒索軟體家族的最新變種。該惡意軟體會加密使用者檔案，並冠上 .Insom 副檔名。檔案名稱也會被變更附加獨特的受害者 ID 和惡意軟體開發者的電子郵件位址。惡意軟體具有從受感染端點移除陰影複本的功能。Insom 會以一個名為「README-WARNING.txt」文字檔形式留下勒索贖金支付說明，提示受害者透過提供的電子郵件位址與攻擊者聯絡。

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：

- Ransom.Makop!g1
- WS.SecurityRisk.4

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/08/22

錢之所在就是詐騙天堂～針對美國駕駛人的過路費網路釣魚詐騙日益增加

美國有四通八達的收費道路、橋樑和隧道，收費服務用於基礎設施的維護和發展，而不需完全依賴州和聯邦的稅收。每天都有數百萬的駕駛使用收費道路，其中許多人選擇使用電子收費 (ETC) 系統，因為它提供了便利性，而且通常還提供折扣費率。根據市調機構 IMARC(the International Market Analysis Research and Consulting Group) 的資料，2023 年 ETC 市場價值為 31 億美元，並預期持續成長。

這項蓬勃發展的服務，以及其不斷成長的使用者族群和涉及大量金流，網路犯罪分子當然不會放過。越來越多的網路釣魚和詐騙行動被觀察到，特別是在手機上透過惡意簡訊進行的詐騙行為。在過去幾週，賽門鐵克發現有多個團體和個人冒充各種美國收費服務系統。惡意簡訊經過精心設計以製造急迫感，並包含一個惡意網址，透過錯別字 (打錯字) 的域名或模仿合法收費服務的類似域名 (typo-squatting)，這是一種突出的策略，犯罪分子註冊拼寫錯誤或相似外觀的域名，以誘使用者瀏覽假網站。

繳費期限前的催收通知特有的急迫性成為網路釣魚攻擊的利器。使用者擔心潛在的付款問題或服務中斷，因此更有可能匆忙回應網路釣魚嘗試，讓攻擊者迅速取得敏感資訊或誘使他們支付偽造的帳單。

近期惡意簡訊的範例：

- Texas Tolls Services，our records show that your vehicle has an outstanding toll charge. To prevent further fees totaling $117.50, please set- tle the due amount of $11.75 at hxxps[:]//rmatollservices[.]com *德克薩斯州收費服務，我們的記錄顯示您的車輛有未付的通行費。為了避免進一步的費用，總計 $117.50，請透過以下網址 hxxps[:]//rmatollservices[.]com 結清 $11.75 的應付金額。
- Illinois Tollway Services, our records indicate that your vehicle has an unpaid toll invoice. To avoid additional charges of $52.90, please settle your balance of $5.29 at illinoistollwayinvoice[.]com *伊利諾州收費公路服務，我們的記錄顯示您的車輛有一張未付的收費發票。為避免 52.90 美元的額外收費，請透過以下網址 illinoistollwayinvoice[.]com 結清 5.29 美元的餘額。
- Florida Turnpike, our records indicate that your vehicle has an unpaid toll invoice. To avoid additional charges

of $68.90 please settle your balance of $6.89 at hxxps[:]//sunpassinvoice[.]com. *佛羅里達州收費公路，我們的記錄顯示您的車輛有一張未付的通行費發票。為了避免額外收費 68.90 美元，請透過以下網址 hxxps[:]//sunpassinvoice[.]com 結清您的 6.89 美元餘額。

- North Carolina Tolls Services, our records indicate that your vehicle has an unpaid toll invoice. To avoid additional charges of $76.00, please settle your balance of $7.60 at hxxps[:]//ncquickpasstolls[.]com *北卡羅萊納州通行費服務，我們的記錄顯示您的車輛有未付通行費發票。為避免 76.00 美元的額外收費，請透過以下網址 hxxps[:]//ncquickpasstolls[.]com 結清 7.60 美元的餘額。
- Pennsylvania Turnpike Tolls. Services, our records indicate that your vehicle has an unpaid toll invoice. To avoid additional charges of $86.00, please settle your balance of $8.60 at hxxps[:]//paturnpiketollbill[.]com *賓夕法尼亞州收費公路。服務，我們的記錄顯示您的車輛有一張未付的通行費發票。為了避免額外收費 86.00 美元，請透過以下網址 hxxps[:]//paturnpiketollbill[.]com 結清您的 8.60 美元餘額。
- Our records indicate that your vehicle has used the FasTrak Express Lane. To avoid additional charges of $55.90, please settle your balance of $5.59 at hxxps[:]//tollbayareafastrak[.]com *我們的記錄顯示您的車輛使用了 FasTrak 快速車道。為避免 55.90 美元的額外收費，請透過以下網址 hxxps[:]//tollbayareafastrak[.]com 結算您的 5.59 美元餘額。
- Washington mygoodtogo tolls services, our records indicate that your vehicle has an unpaid toll invoice. To avoid additional charges of $66.70 please settle your balance of $6.67 at hxxps[:]//mygoodtogotoll[.]com *您好，根據我們的記錄，您的車輛有一張欠繳的通行費。為了避免額外收取 66.70 美元的費用，請透過以下網址 hxxps[:]//mygoodtogotoll[.]com 結清您的 6.67 美元餘額。

整體而言，收費服務已成為社交工程詐騙攻擊覬覦的目標，同時影響消費者和企業。雖然這些攻擊在美國不斷增加，但其他國家如澳洲、加拿大和日本也受到影響。

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-SESE/**SESC** 有包含這個功能) 也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。WebPulse 已經知道這些攻擊活動中使用的惡意網域。閱讀更多資訊：

- 偵測與防護惡意簡訊
- iOS 裝置上啟用 SMS 過濾延伸功能
- 在 Android 裝置上啟用 SMS 網路釣魚偵測

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。

2024/08/21

TodoSwift惡意軟體：偽裝成PDF全新macOS威脅

一個被稱為 TodoSwift 的 macOS 平台上全新惡意軟體被確認偽裝成 PDF 下載。此威脅份子可能來自北韓，使用 Swift／SwiftUI 開發該惡意植入程式。該惡意植入程式看起來很像一個與比

特幣價格有關看似合法的 PDF 來欺騙用戶。作為其攻擊媒介／手法的一部分，該惡意程式濫用 Google Drive 網址並內嵌命令和控制 (C&C) 的網址作為啟動參數。惡意軟體利用 NSTask 物件來執行具有特定旗標和參數的 curl 指令，以擷取第二階段有效酬載。

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：

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：

- Downloader
- OSX.Trojan.Gen.2
- 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。

2024/08/21

來自北韓威脅份子開發：MoonPeak遠端存取與木馬(RAT)

MoonPeak 是最近發現的遠端存取與木馬(RAT)，據說是來自北韓的威脅份子所開發。此 RAT 是源於開放原始碼 XenoRAT 惡意軟體的後繼變種，並已經過多次演變。思科旗下資安公司 Cisco Talos 研究人員已發表 MoonPeak 的分析報告，以及相關威脅份子基礎設施的分析。

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!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：

- Backdoor.Ratenjay
- Trojan Horse
- Trojan.Gen.MBT

- Scr.Malcode!gdn14
- 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。

2024/08/21

惡意垃圾郵件鎖定義大利銀行業，散佈Quasar(又稱BlotchyQuasar)遠端存取木馬(RAT)

威脅研究人員最近觀察到一個散佈遠端存取木馬 (RAT) 的垃圾郵件攻擊行動，其主要目標是義大利。該行動使用仿冒內政部官方通訊的欺騙性電子郵件，並附有內政部的標誌。雖然惡意軟體和 C&C 伺服器仍然相同，但下載惡意檔案的網址已更新。該惡意軟體特別鎖定某些義大利銀行的客戶。

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：

- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan Horse
- Web.Reputation.3
- WS.Malware.1
- WS.SecurityRisk.4

2024/08/21

網路罪犯瘋狂利用虛假履歷攻破企業防線

網路威脅領域充斥著五花八門的社交工程伎倆，雖然這些伎倆一直在不斷變化，但有些方法是屢試不爽，例如：寄送虛假履歷。這種手法包括以電子郵件寄送虛假的履歷 (CV) 和動機信 (Motivation Letter)，通常以人力資源部門或經理為目標。

網路知識：CV 是 Curriculum Vitae 的縮寫，和 Resume 並不相同。雖然都要用來介紹自己的經歷、為什麼適合這份職位，在台灣也時常被混用，但實際上公司希望看到的內容仍有差別。

採用這種伎倆的惡意垃圾郵件行動屢見不鮮，主要有兩個原因。首先，人力資源專業人員習慣於定期接收求職申請。這些習以為常的例行流程會降低他們的警覺性，使他們更有可能在沒有仔細檢查的情況下打開附件。其次，快速審核潛在應徵者的衝動可能導致匆忙開啟附件，尤其是在時間緊迫或處理大量申請時。

最近案例中，賽門鐵克觀察到一個威脅者向包括美國、英國、加拿大、比利時、印度、澳大利亞、荷蘭、芬蘭、烏克蘭等國家的公司發送電子郵件 (主旨：CV[已刪除的姓名]//求職申請)。

該電子郵件包括一封簡短的動機信 (Motivation Letter)，威脅份子假扮成求職者，強調在行政、財務和會計系統方面的經驗，並表示希望轉任商業職位。附加在電子郵件中是一個惡意壓縮檔 (CV [name removed].zip)，其中包含一個偽裝成履歷的 Formbook(一種常見的惡意竊密程式／表單竊密程式) 二進位檔案。

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：

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：

- Scr.Malcode!gdn33

2024/08/20
防護亮點：防護Linux供應鏈攻擊的第一選擇～賽門鐵克重要主機防護系統：DCS～Data Center Security

Linux 是資料中心作業系統的首選，因為它具有多項關鍵優勢，包括可擴充性及可靠性、安全性、自訂性、效能及成本效益。但這些系統並無法隨時跟上建議的安全修補程式，且這些修補程式的發佈頻率越來越高。這些系統也經常執行舊的應用程式，廠商的安全修補程式可能無法使用，或者為了維持業務連續性，系統可能根本不會排定修補程式更新的時間，而修補程式停機無法滿足持續營運計畫 (BCP：Business Continuity Planning)。因此，資料中心環境受到網路攻擊和供應鏈攻擊的風險可能非常高。攻破單一資料中心可存取多個相互連線的系統和應用程式，使攻擊的潛在風險難以估計。

供應鏈攻擊是惡意軟體設計者和進階持續性威脅 (APT) 駭客組織為了在其目標主機或系統中取得一席之地而採用的顯著「初始存取」策略。此方法涉及攻擊目標信任第三方服務或軟體，並將惡意程式碼注入合法的軟體更新或發行版本。

Linux.Gomir後門程式

賽門鐵克的威脅獵手團隊 (Threat Hunter Team) 發現一個由北韓 Springtail 間諜組織 (又名 Kimsuky) 所開發的全新 Linux後門，該後門與最近一次針對南韓組織攻擊行動中使用的惡意軟體有關。該後門 (Linux.Gomir) 應該是 GoBear 後門的 Linux 版本，GoBear 後門被用於最近 Springtail 的攻擊行動中，攻擊者透過特洛伊木馬化的軟體安裝套件傳送惡意軟體。Gomir 在結構上幾乎與 GoBear 完全相同，兩者之間存在大量共用的程式碼。

Kimsuky 也稱為 Velvet Chollima，是北韓的進階持續威脅 (APT) 駭客組織，主要從事網路間諜行為。自 2012 年左右出現以來，Kimsuky 已針對韓國、日本、美國和多個歐洲國家的單位進行攻擊。該組織擅長開採濫用常用軟體中的漏洞，利用零時差漏洞和已知的安全漏洞來滲透系統。這起事件突顯保護軟體供應鏈安全的重要性，因為即使是可信賴的軟體，如果在其散佈或傳遞更新過程中的任何階段受到攻擊，也可能成為複雜網路攻擊的媒介。

賽門鐵克重要主機防護系統：DCS~Data Center Security有效解決方案

賽門鐵克重要主機防護系統：DCS～Data Center Security 提供全面深度的防護方法，以確保 Linux 伺服器的安全與防護。我們的解決方案能有效提供零時差防護，以對抗日益猖獗的供應鏈攻擊和其他針對 Linux 資料中心環境的網路威脅。

專為UNIX資料中心提供DCS內建強化政策

其出廠就內建的 Unix 保護政策，底層邏輯是最小權限／最少資源原則，可鎖定 Linux 資料中心。DCS 的亮點在於它能夠拆解 Gomir 攻擊鏈的每一步驟並在每個步驟都提供完善的保護。

初始存取

Gomir 惡意軟體支援從遠端伺服器接收指令的執行功能，據說是透過偽裝成韓國運輸組織應用程式的假驅動程式進行傳播。DCS 網路控制可將用戶端應用程式的邊界定義為可信賴的網路和裝置，進而限制初始存取。此外，您也可以僅允許在特定連接埠上進行網路連接。

惡意軟體執行

在 DCS 強化 Linux 伺服器中軟體執行控制可禁止惡意軟體從 temp 或其他可寫入位置執行。

持續性／常駐功能

持續性機制取決於 syscall 202 或 getegid32() 呼叫的輸出。如果程序的群組 ID 在 root 下執行，範例會將自己安裝在 crontab 或 systemd 服務中。

- **CronTab**

  範例將嘗試將其安裝到現有的 crontab 中。樣本首先會透過本機 shell 使用「crontab -l」指令取得現有的 cron 紀錄。命令輸出將被複製到新的 cron 緩衝區。此緩衝區包含新的 cron 記錄「@reboot <可執行檔路徑>」。

  新的 cron 排程為其持續機制，在系統重啟時會啟動/重啟該程序。cron 標籤項目會儲存在檔名為「cron.txt」的暫存檔中，此檔案會作為「crontab」指令的第一個參數導入。一旦 crontab 更新新項目，'cron.txt' 就會被刪除。

  在 DCS 強化的 Linux 伺服器中，軟體安裝限制和作業系統限制會阻止建立新的 crontab。

- **Systemd 服務**

  範例會取得其目前執行的可執行路徑，並在 '/var/log/syslogd' 中建立副本。在 '/etc/systemd/system/' 目錄中建立一個新的 systemd' 服務。該檔名為「syslogd.service」。這是用來混淆系統管理員，讓他們忽略這個服務，它會指向一個假的 '/var/log/syslogd'，也就是目前正在執行的樣本。這個新的服務檔案會讓 Gomir 在重新啟動系統時執行，並確保在『network』項目之後載入。這表示後門將有能力存取已初始化的網路介面。經 DCS 強化過的 Linux 伺服器中，軟體安裝限制和作業系統限制會阻止建立新的服務或服務設定檔。

指令與控制

本範例將透過 HTTP 使用硬體編碼的 IP 和 URL。本範例使用 HTTP 發送請求來執行指令，並將結果傳送至 C2 基礎架構。C2 可在樣本中 '.rodata 部分的 0x0834F79F' 位址找到。命令以整數值組成，表示要執行的命令類型。這部份很容易被威脅者變更，而有效負載格式的結構是四個位元組的加密金鑰和長度可變的指令。DCS 網路控制可以拒絕所有傳入或傳出的網路連線。此外，您也可以僅允許特定連接埠的網路連線。

解析Linux.Gomir採用TTPs在MITRE ATT&CK框架上的分類

Symantec DCS 提供下列 TTPs(策略、技術與程序) 的預設防護：

- TA0001 初始存取
- TA0002 執行
- TA0003 持續性
- TA0004 權限提升
- TA0005 防護規避
- TA0007 搜尋
- TA0009 收集
- TA0010 滲漏
- TA0011 指揮與控制
- TA0040 影響
- T1005 本機系統資料
- T1036 偽裝
- T1053 排程任務／工作
- T1053.003 Cron
- T1059 命令和腳本編譯器
- T1070 指示符移除
- T1070.004 檔案刪除
- T1071 應用層通訊協定
- T1071.001 網路通訊協定
- T1189 偷渡式入侵
- T1204 使用者執行
- T1204.002 惡意檔案
- T1217 瀏覽器資訊搜尋
- T1529 系統關機／重新開機

- T1543 建立或修改系統程序
- T1543.002 Systemd 服務
- T1546 事件觸發執行
- T1546.016 安裝套件

保護資料中心的環境是重中之重

企業必須優先採取安全措施，包括及時修補程式、強大的存取控制和持續監控，以降低供應鏈攻擊的風險，並保護敏感資料不被探刺利用。賽門鐵克重要主機防護系統：DCS～Data Center Security 其出廠就內建許多預設政策可套用，可確保提供強大的防護，避免資料中心伺服器和工作負載遭受不斷增加的入侵點探刺利用攻擊。

關於賽門鐵克的重要主機防護系統：DCS～Data Center Security 的完整資訊可點擊網頁說明或最新簡報檔。網頁或簡報如有說明不夠清楚的地方，歡迎與保安資訊的業務或技術顧問提供建議。

2024/08/20

QWERTY：全新的惡意竊密程式

QWERTY 是全新發現的惡意竊密程式，被觀察到上架保存在一個位於德國 Linux 虛擬專用伺服器上，該伺服器同時提供某些服務。該惡意軟體能夠在執行前執行各種檢查，以檢查是否存在偵錯或虛擬化環境，並具有下載其他後續有效酬載的能力。QWERTY 目標是擷取儲存在各種網頁瀏覽器中的系統資訊和資料，並隨後將收集到的資訊滲出到攻擊者所操控 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：

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.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。

2024/08/20

Styx惡意竊密軟體

Styx 惡意竊密軟體是 Checkpoint 研究人員發現一種全新的惡意竊密程式。該惡意軟體具有從基於 Chromium 瀏覽器中滲出各種資料的功能，包括 Cookie、憑證、銀行詳細資料、加密貨幣錢包、預先已定義的副檔名的檔案、Telegram 和 Discord sessions 等。SStyx 惡意竊密軟體被認為是源於較舊的惡意竊密軟體：Phemedrone 後繼變種。該惡意軟體在網路上進行廣告宣傳，並透過訂閱模式銷售。Styx 採用多種沙箱迴避與反分析技術，包括檢查執行中除錯工具或與虛擬環境相關的程序。

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.MalTraffic!gen1
- SONAR.Stealer!gen1
- 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.Malcode!gdn14
- Trojan Horse
- 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

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
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564

- System Infected: Trojan.Backdoor Activity 654
- 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。

2024/08/20

透過DNS流量進行通訊全新Msupedge後門程式：已有台灣某大學遭受攻擊

在針對台灣一所大學攻擊中，被部署一個先前未見過的後門 (Backdoor.Msupedge)，利用一種不常見的技術。此後門最顯著的特徵是透過 DNS 流量與命令與控制 (C&C) 伺服器通訊。儘管這種技術已廣為人知，並曾被多個威脅份子使用，但並不常見。

我們部落格文章有更詳細的報導：針對台灣攻擊的新後門採用隱匿的通訊方式。

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.Ps-Enc!g1
- ACM.Ps-Rd32!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：

- Backdoor.Msupedge
- 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!200

2024/08/20

新興惡意軟體：UULoader，鎖定韓語和中文使用者

最近研究觀察到惡意軟體行動採用惡意的 .msi 檔案有增加趨勢，雖然這種檔案並不常見，但卻是已知的惡意軟體散佈方法。新發現的惡意軟體類型是「UULoader」，用來傳送下一階段的有效酬載，例如：Gh0st 遠端存取木馬 (RAT) 和 Mimikatz。它透過偽裝成合法應用程式的惡意安裝程式散佈，主要鎖定韓語和中文使用者。

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
- Trojan.Gen.NPE.C
- Trojan.Gen.2
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/08/19

鎖定越南主要產業：冒充知名石油與天然氣公司傳遞RedLine惡意竊密程式

賽門鐵克最近觀察到一個傳遞 RedLine 惡意竊密程式的惡意垃圾郵件行動，其中一個攻擊者冒充越南一家專門從事勘探和生產活動且居於領導地位的石油和天然氣公司。越南各行各業的本地和跨國公司--包括石油和天然氣、工業、電氣和空調 (HVAC：Heating、Ventilation、Air-conditioning and Cooling) 系統製造商、塗料、化學和酒店業，無一倖免。

惡意電子郵件經過精心製作，看起來像是該石油公司為其一家煉油廠提供更換和維修服務的投標邀請函，邀請收件者確認並遞交報價單，以回應虛構的詢價單 (RFQ)。該電子郵件包含一個惡意的 RAR 壓縮檔附件 (1.No. BDOPS-2024-057_RFQ.rar)，其中包含 RedLine 惡意竊密程式的二進位檔案 (Palace Residences 2024-25.exe)。

RedLine 是一款知名的惡意竊密程式，其目標為登入憑證、信用卡詳細資料、瀏覽器歷史記錄，甚至是加密貨幣錢包。它遭全球許多駭客組織和個體戶大肆濫用。安裝後，它會從受害者的電腦收集資料，並將資料傳送到攻擊者控制的遠端伺服器或 Telegram 頻道。

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.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：

- Scr.Malcode!gdn33

基於機器學習的防禦技術：

- Heur.AdvML.B

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

2024/08/19

Tusk網路攻擊行動：散播多種惡意竊密程式

Danabot 和 StealC 已在最近一系列被稱為「Tusk」網路惡意行動中，被辨識出傳送惡意竊密程式的有效酬載。據報導，攻擊者在攻擊鏈中利用稱為 HijackLoader 的模組化載入程式。惡意下載程式上架存放在 Dropbox 雲端空間，並偽裝成軟體安裝程式或更新套件。傳播的惡意竊密程式有效酬載能夠收集受感染端點的硬體和網路資訊、儲存在網頁瀏覽器或瀏覽器擴充套件中的機密資料、加密貨幣錢包等。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspLaunch!g233
- 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
- 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

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。

2024/08/19

Ailurophile惡意竊密程式

Ailurophile 是最近在真實網路情境中發現一種全新基於 PHP 的惡意竊密程式。該惡意軟體在網路上進行廣告宣傳，並透過訂閱模式銷售。Ailurophiles 功能包括竊取瀏覽器中儲存的資料，包括自動填入資訊、cookie、憑證、銀行詳細資訊、瀏覽歷史和加密貨幣錢包。該惡意竊密程式還可根據預先定義的搜尋準則，例如：檔案名稱中關鍵字或特定的副檔名，從受攻擊機器中滲出資料檔案。

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：

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：

- 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。

2024/08/19

假冒APP鎖定符合印度政府PM Kisan Yojana助農計畫資格的人

PM Kisan Yojana 是印度政府一項歷史性舉措，目前全印度約有八百萬農民受惠。每年符合資格的農民可獲得總額 6,000 盧比獎金，分三期等額發放，每期 2,000 盧比。若要獲得優惠，必須透過 PMKSNY 官方網站進行線上登記。註冊 PM Kisan Yojana 之後，許多農民需要協助更新註冊表上的資訊，包括他們的 Aadhaar 號碼 (一個 12 位數的個人識別碼，可作為印度居民的身分證明和住址證明)、銀行帳戶資訊和手機號碼。

網路知識：在總理 Kisan Yojana 領導下，每年向全國所有符合資格的農民家庭提供 6,000 盧比收入支持，分三期等額發放，每四個月 2,000 盧比。該計劃將家庭定義為丈夫、妻子和未成年子女。 2,000 盧比資金直接轉入農民／農民家庭的銀行帳戶。

網路罪犯利用此更新程序，在社交媒體上散佈 PM Kisan Yojana 助農計畫假冒專用 APP 的連結。點擊這些連結會下載惡意安卓平台 APP (例如：PM KISAN YOJANA.apk)。一旦安裝並執行，該 APP 會顯示一個模仿印度銀行標誌的表單，要求用戶輸入手機號碼、MPIN、銀行卡號細項資訊等資訊。此外該 APP 還能竊取手機簡訊內容，可能會因洩露個人和銀行資訊而導致財務損失。

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

2024/08/19

Hawk Eye勒索軟體

有人在真實網路情境中觀察到一種名為「Hawk Eye」的勒索軟體。被加密後檔案會隨機冠上 4 個字元的副檔名。勒索贖金支付說明文字檔 (read_it.txt) 會被放在不同的資料夾中，桌布也會變為黑底的白鷹。根據勒索贖金支付說明文字檔的內容，會採用雙重勒索手法，即除了加密檔案外，攻擊者還會告知使用者資料已外流，如果不支付贖金，資料就會外洩或被販賣。

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.SuspBeh!gen625
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2024/08/18

冒充特斯拉的加密貨幣投資詐騙

最近的一份報告顯示，網路騙子正在冒用特斯拉的名義來進行加密貨幣詐騙。這些騙徒註冊了包含「Tesla」的網域，以欺騙使用者落入瀏覽惡意連結的陷阱。這些連結會誘導下載有害的安卓APP，並在 YouTube 和 Telegram 等社交平台上進行宣傳。

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

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。

2024/08/16

威脅份子：Damselfly針對美國和以色列發動網路攻擊行動

Damselfy駭客組織 (也稱為 APT42，Charming Kitten) 是一個以伊朗為基地的知名威脅份子。該組織經常攻擊美國和以色列的高價值目標。這些攻擊主要目標是竊取非政府組織及學術、政府、國防／軍事組織等單位的憑證，以進行伊朗本身的軍事和政治理想。觀察到憑證釣魚行動使用社交工程設計的誘餌，並利用連結、假網站和公開可用的服務，例如：Dropbox、OneDrive 和 Google 提供的服務。

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-Http!g2
- 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：

- Downloader
- Infostealer
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.4

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。

2024/08/16
BANSHEE全新macOS惡意竊密程式

就在本月一種名為「BANSHEE 」全新 macOS 惡意竊密程式被發現，它是由俄羅斯威脅份子所製造。它會影響 x86_64 和 ARM64 macOS 系統，並針對重要的系統資訊、瀏覽器資料和加密貨幣錢包造成重大威脅。

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：

- 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。

2024/08/16
在真實網路情境上觀察到全新的Gafgyt殭屍網路

在真實網路情境上觀察到一個全新的 Gafgyt 殭屍網路。此惡意軟體是以 SSH 認證薄弱的端點為目標進行散佈，並部署兩個不同的 ELF 二進位檔。其中一個檔案是 Go 語言 的 Gafgyt 二進位檔，具有各種功能，包括系統搜尋、指令執行、掃描暴露的 SSH／Telnet 存取以及對目標系統執行暴力攻擊。第二個二進位檔是 XMRig 挖礦程式，用於挖掘 Monero 加密貨幣。

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：

- Miner.XMRig
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

2024/08/16

全新的ValleyRAT遠端存取木馬涉入惡意軟體散佈行動

Fortinet 研究人員報告一個針對中文使用者的全新 ValleyRAT 遠端存取木馬散佈行動。此行動背後的攻擊者依賴各種元件，包括為反射 DLL 載入而執行的 shellcode，以及用於擷取其他元件的定位模組。該行動的有效酬載--ValleyRAT 是一個多階段的惡意軟體，其功能包括監控用戶活動、擷取螢幕截圖、執行外掛程式、下載任意檔案等。

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。

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。

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**。