保安資訊--本周(台灣時間2023/12/08)
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 60 萬 9,300 台受保護端點上總共阻止了 7,090 萬次攻擊。這些攻擊中有 81.6% 在感染階段前就被有效阻止：**(2023/12/04)**

- 在**10萬9,100**台端點上，阻止了**2,610**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**17萬3,500**台端點上，阻止了**1,480**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬2,800**台**Windows**伺服主機上，阻止了**1,180**萬次攻擊。
- 在**6萬4,800**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,800**台端點上，阻止了**92萬3,300**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,800**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**23萬200**台端點上，阻止了**410**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,600**台端點上，阻止了**410**萬次加密貨幣挖礦攻擊。
- 在**11萬9,500**台端點上，阻止了**900**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**828**台端點上，阻止了**13萬1,100**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 1.441 萬個受保護端點上阻止了總計 610 萬次攻擊。**(2023/12/03)**

- 使用網頁信譽情資，在 **1.273** 萬個端點上阻止 **520** 萬次攻擊。
- 攔截 **31.1K** 個端點上 **613.1K** 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 **13.1K** 個端點上攔截 **169.8K** 次瀏覽器通知詐騙攻擊。
- 在 **624** 個端點上攔截 **56K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。
- 在 **1.3K** 個端點上阻止 **2K** 次技術支援詐騙攻擊。
- 在 **221** 個端點上阻止 **858** 次加密劫持嘗試。

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。

2023/12/06

小心隨身碟容易感染的～Vetta(*維塔)惡意程式載入程式

Vetta 惡意程式載入程式 (Loader) 是一種新發現，藉由受感染的 USB 隨身碟傳播惡意軟體。在針對義大利各行業部門的攻擊行動中發現該惡意軟體。初始感染鏈是利用遭感染設備上的捷徑檔 (*.lnk)、PowerShell 腳本來進一步傳播保存在分影音分享網站上的惡意腳本，最終實現 Vetta Loader 有效籌載的交付。迄今為止，至少發現四種不同的 Vetta Loader 變種，各自使用下列不同程式語言所撰寫： NodeJS、Golang、Python 和 .NET。

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：

- ACM.Ps-Net!g1
- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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.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：

- System Infected: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 721
- 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。

2023/12/06

NovaSentinel(*新星哨兵)竊密惡意程式

賽門鐵克持續監控威脅環境中新出現的威脅，我們每天都會監控到許多威脅。雖然有些威脅最終無疾而終，但有些威脅卻長盛不衰。在本防護公報中，我們將簡要介紹最近發現一個威脅及其測試相關的活動。

這種威脅被稱為 NovaSentinel，是一種典型的竊密惡意程式，主要用於竊取遊戲玩家和加密貨幣愛好者的資訊，但也有能力入侵企業。它目前的售價為每月 250 歐元，終身使用權為 3040 歐元。以下是其主要功能概述：

- 竊取各種線上遊戲的連線資訊（EpicGames、RiotGames、Growtopia、Ubisoft）
- 接管 Discord 帳戶
- 竊取敏感的瀏覽器相關資訊（cookie、密碼、歷程記錄、書簽、自動填表資訊、保存的信用卡）
- 竊取加密貨幣錢包
- 收集 Filezilla、Putty、TotalCommander 伺服器資訊
- 搜刮檔案

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer

2023/12/06

開採濫用ProxyShell漏洞打造的ProxyShellMiner挖礦軟體攻擊活動明顯增加

最近，我們在特定的 IPS 特徵類別中出現偵測到高峰。經過進一步分析，我們發現該行為與 ProxyShellMiner 有關。據觀察，攻擊者利用 Windows Exchange 伺服器中 ProxyShell 漏洞 CVE-2021-34473 和 CVE-2021-34523 成功滲透到組織的網路後，就會在受害者系統上植入該挖礦軟體。ProxyShellMiner 使用一種稱為行程掏空 (process hollowing) 技術，將挖礦程式注入被入侵系統上的瀏覽器，並啟動挖礦程序。ProxyShellMiner 可導致服務中斷、伺服器性能下降和營運的網路中斷。一旦攻擊者取得網路存取權限，他們就可以執行更多的惡意行為，例如：後門部署或遠端程式碼執行。

賽門鐵克的網路保護技術入侵防禦系統 (IPS) 會阻止這種挖幣活動，以防止對系統造成破壞。IPS 還能阻止開採濫用 ProxyShell 漏洞的嘗試。

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：

- System Infected: Trojan.Coinminer Activity 32
- Web Attack: Microsoft Exchange Server CVE-2021-34473
- Web Attack: Microsoft Exchange Server Elevation of Privilege CVE-2021-34523
- Web Attack: Microsoft Exchange Server RCE CVE-2021-34473

2023/12/06

SpyNote(*間諜筆記)網路攻擊行動：鎖定巴西農業為攻擊目標

賽門鐵克已經發現一名冒充 AgroPart(一家為農業提供農機零件備品服務的專業公司) 的威脅行動者，以巴西農民為目標。

他們將 SpyNote 惡意軟體 (Agro-Partes.apk) 偽裝成 AgroPart 的專用手機 APP，企圖引誘使用者安裝。這種威脅已經存在好幾年，其原始程式碼已向公眾開放，並不斷被世界各地的多個駭客組織和個人使用。

以下是其會收集的資訊內容：

- 按鍵
- 設備資訊
- 連絡人
- 通話記錄和簡訊
- 照片和影片
- 已安裝APP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：

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

2023/12/06

搭便車～macOS平台上出現多種盜版軟體暗藏惡意軟體大肆傳播

在真實網路情境觀察到一起針對 macOS 平臺散播惡意軟體的全新攻擊行動。攻擊者將惡意軟體二進位檔案偽裝成 4K Video Downloader、Aiseesoft Mac Video Converter、MacX Video Converter Pro、Sketch Wondershare UniConverter 等破解／盜版應用程式的 .pkg 安裝包。一旦入侵電腦器，植入的木馬就會連線到攻擊者所操控的 C&C 伺服器，並等待進一步的指令。據瞭解，使用的 C&C 伺服器已被其他一些用於 Android 和 Windows 平臺的惡意樣本所使用，這顯示該攻擊行動的範圍可能不僅限於 macOS 設備。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Android.Malapp
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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：

- System Infected: Trojan.Backdoor Activity 634

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。

2023/12/06

CISA有通報喔～Adobe ColdFusion CVE-2023-26360漏洞正被大肆開採利用

Adobe ColdFusion 存在一個不正確的存取控制漏洞 (CVE-2023-26360，CVSS 風險評分無 8.6)。如果被成功開採濫用，該漏洞可允許遠端程式碼執行。美國網路安全及基礎設施安全局 (Cybersecurity and Infrastructure Security Agency，CISA) 最新網路安全通報特別揭露針對政府機構的漏洞利用攻擊的實例。拆解攻擊者的攻擊鏈發現在偵察和資料滲出階段有使用量身打造的遠端存取木馬 (RAT) 和惡意網頁殼層 (Web Shell)。

賽門鐵克的網路保護技術入侵防禦系統 (IPS) 可阻止開採濫用 CVE-2023-26360 漏洞的企圖，進而防止系統受到進一步感染／入侵。

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

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：

- Attack: Adobe ColdFusion Unauthenticated RCE CVE-2023-26360

2023/12/06

網路釣魚攻擊行動：針對 Truist 銀行客戶的手機簡訊釣魚行動

在世界各地，大家對大型銀行的客戶所遭受的網路釣魚攻擊習以為常，但我們不能忘記地區性銀行也不斷成為攻擊目標。例如：Truist (主要在美國東南部和大西洋中部地區運營) 客戶不斷收到惡意簡訊，假借他們帳戶已被凍結，並建議他們按照提供的網址進行驗證。毫無戒心的用戶會被引誘到一個假冒 Truist 網站，該網站專門用來進行網路釣魚。

觀察到的簡訊內容樣本：

- Truist-Alert^sca5v.zw69:For your protection we have placed a hold on your account.visit hxxps[:]//cebabh[.]edu[.]pe/truist/ to verify.

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。Webpulse(網頁脈衝) 的網頁安全防護機制已將假冒的 Truist 網站歸類為不安全。

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。

2023/12/05

以Netflix為幌子的網路釣魚和詐騙持續存在

自從 Netflix 網路隨選串流影片在全球大受歡迎以來，針對全球使用者的網路釣魚和詐騙行為就層出不窮。這些惡意攻擊行動每天都在發生，其中大多數源自惡意電子郵件，而手機簡訊詐騙也日益不惶多讓。

最近幾個星期，賽門鐵克發現有人向手機用戶發送惡意簡訊。這些簡訊試圖誘騙用戶相信他們的 Netflix 帳戶可能被註銷，並敦促他們點擊所提供的網址來解決問題。在另一種情況下，使用者會受到虛假支付問題的引誘。

觀察到的惡意簡訊樣本：

- Netflix 付款方式暫停。請確認您的詳細資訊以避免帳戶被取消：hxxps[:]//prefilenotice[.〕
- Netflix 帳戶擱置。請確認您的詳細資訊，以免帳戶被取消：hxxps[:]//profilenotice[.〕
- Netflix：您的付款無法完成。要繼續使用服務，請訪問 hxxps[:]//Netflix-subcription[.]com 以更新您的付款方式。
- Netflix：Votre compte est temporairement suspendu en raison d'un problème avec votre dernier paiement. 如需瞭解您的付款方式，請訪問：hxxps[:]//compteresoudre-netflix[.〕

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。Webpulse(網頁脈衝) 的網頁安全防護機制已將假冒的 Netflix 網站歸類為不安全。

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。

2023/12/05

TrickMo手機版的網路銀行木馬

TrickMo 是一種手機版的網路銀行木馬，最早發現於 2019 年。該惡意軟體的後繼變種在最近的惡意攻擊行動中大肆傳播。TrickMo 現在具有一些新功能，包括螢幕擷取、下載附加模組、執行命令和 HTML 覆蓋注入等。TrickMo 繼續專注於竊取各種銀行和加密貨幣相關憑證和資料。該惡意軟體的主要目標是各種眾所周知的網路銀行系統、加密貨幣錢包，但也包括電子郵件、購物和社交媒體應用程式。

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：

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。

2023/12/05

濫用DCRAT遠端存取木馬(RAT)的網路攻擊行動：土耳其境內的機構組織正遭受蹂躪

DCRAT (又稱『Dark Crystal--黑暗水晶』) 遠端存取木馬 (RAT)，至少從 2019 年就開始出現了，在過去幾年中時而出現流行高峰。在當今的威脅形勢下，它的流行程度有所降低，但仍能觀察到零星的活動。

在最近一個例子中，賽門鐵克阻止一個針對土耳其組織的攻擊行動。惡意攻擊者使用夾帶惡意 XLA 檔案 (Hesap bildirimi.xla) 的惡意垃圾郵件 (主旨：Hesap bildirimi)，該檔案會從特定網站下載 DCRAT 惡意有效籌載 (server1.exe)。

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：

- ISB.Downloader!gen60

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。

2023/12/05

防護亮點：讓數據說話～賽門鐵克的Webpulse(網頁脈衝)網頁安全防護生態系統上個月的防護績效？

Symantec WebPulse (網頁脈衝) 網頁安全防護機制是業界最佳的網路安全引擎，可為包括財富 500 強企業和消費者在內的數億客戶設備提供保護。

WebPulse 是賽門鐵克全球資安情資網路 (GIN：Symantec Global Intelligence Network) 的重要成員，是一種架構在雲端基礎架構，由使用者行為驅動的強大力量，能將使用者瀏覽網頁的最新狀態轉化為全球網頁分類／過濾／安全的大數據庫與威脅情資。

WebPulse 採用多種技術對輸入內容進行分析，是業界最快、最精準的網頁分類和風險評級。在 WebPulse 框架內，每個回饋到 WebPulse 生態系統的網頁都要經過多種不同威脅分析方法 (包括自動和手動) 的處理。

在過去的 30 天裡，WebPulse 總共阻止 7.77 億次不同安全類別的攻擊。

＊請注意，這些統計數據僅呈現網頁分類／過濾／安全的雲端服務，並不包括企業內部的 BlueCoat Proxy SG……等網頁分類／過濾／安全的自建系統的績效。

- 可疑類別：4.56 億
- 惡意來源／惡意網路類別：1.73 億
- 網路釣魚類別：4,900 萬
- 遭入侵操控網站類別：2,500 萬
- 惡意離埠資料／殭屍網路類別：2,200 萬
- 詐騙／可疑的合法網站類別：2,100 萬
- 垃圾郵件類別：1,700 萬
- 潛在不需要的軟體類別：1,400萬

建議賽門鐵克網頁防護 8 合1套件組合 (WPS) 用戶啟用 WebPulse 即時分類，以獲得最佳保護。按一下此處獲取有關設定 WebPulse 的說明。

##保安特別說明：較新版本的端點防護 (SEP) 已免費整合賽門鐵克網頁防護的部分功能，其實也是受益於 WebPulse 網頁安全防護生態系統隨時都在更新的網頁情資大數據。還在使用較舊版本的用戶，可評估升級的可行性。

點擊此處瞭解賽門鐵克網頁安全防護引擎及生態雲端系統：WebPulse 的更多相關資訊。

2023/12/05

RA World勒索軟體

最近在真實網路情境發現 RA World 是另一種露出檯面的勒索軟體，它會加密用戶檔案並冠上 .RAWLD 副檔名。受害者會被提示透過 Tox 或 Telegram 聯繫攻擊者，以取得如何解密的協助。檔名為『Data breach warning.txt』的勒索 (贖金支付) 說明檔案警告說，如果不乖乖付贖金，就要脅公開已竊取的資料。RA World 勒索軟體會刪除遭感染系統上的磁卷陰影複製 (volume shadow copies)。

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.Ransomware!g1
- SONAR.Ransomware!g3
- SONAR.Ransomware!g7
- SONAR.Ransomware!g38
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253

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

2023/12/05

檔案共享平臺ownCloud的graphapi元件嚴重等級漏洞：CVE-2023-49103正遭受大肆開採濫用

CVE-2023-49103 是一個被正式揭露 ownCloud Graph API 擴展的嚴重等級 (CVSS 得分 10.0)。成功開採利用該漏洞可能會洩露敏感性資料，包括管理員憑據。我們注意到有報告顯示，該漏洞在真實網路情日益被大肆開採利用。賽門鐵克的網路防護技術入侵防禦系統 (IPS) 可阻止這些漏洞利用嘗試，以防止對系統造成進一步感染／入侵。

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: ownCloud graphapi Information Disclosure Vulnerability CVE-2023-49103

2023/12/04

Qilin(*麒麟)勒索軟體的Linux平台版本正在鎖定VMware ESXi

Qilin 勒索軟體又名 Agenda，最初發現於去年，最初主要針對 Windows 的環境。最近在真實網路情境也觀察到這種惡意軟體已經有 Linux 平台的新版本，據報導其目標是針對 VMware ESXi 環境。該惡意軟體具有較多的設定功能可依需選用，允許只對特定檔案類型進行選擇性加密，並可指定不包括在加密範圍內的排外資料夾。Qilin 還具有終止特定系統程序和運行中虛擬機器的功能，以及額外對虛擬機器快照進行加密的額外自訂的選項。

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：

- Ransom.Qilin
- WS.SecurityRisk.4

2023/12/04

Cactus(*仙人掌)勒索軟體

Cactus 索軟軟體，最早發現在 2023 年 3 月前後。最近，該惡意軟體正在利用資料分析系統 Qlik Sense 的漏洞利用攻擊行動中以及透過利用 Danabot 惡意軟體的惡意廣告散播行動進行傳播。據瞭解，Cactus 會使用 RDP 協議或各種遠端存取工具在遭入侵環境中進行橫向移動。檔案被加密後，惡意軟體會以名為『cAcTuS.readme.txt』的文字檔形式發送勒索 (贖金支付) 說明，建議受害者透過指定的電子郵寄地址與攻擊者聯繫。該勒索軟體背後的威脅行動者還會試圖在檔案加密前竊取使用者資料。為此，他們會使用 Rclone 的開源資料備份等工具複製並竊取受害組織的資料以利後續 (如不付贖金) 施展不付錢就將資料公開的雙重勒索戰略。

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：

- AGR.Terminate!g2
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Cactus
- 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

2023/12/04

後門程式Agent Racoon(*浣熊)

在一系列針對中東、非洲和美國不同組織的相關攻擊中，一個名為『Agent Racoon』的新後門惡意軟體被推出。這些攻擊中使用的其他惡意工具包括另一個模仿 Windows 網路提供者元件的 DLL 竊資軟體 Ntospy，以及一個名為 Mimilite 可量身打造功能的 Mimikatz。 Mimikatz 原先是一套 windows 系統中的安全測試工具，後來被大量濫用成為 windows 密碼獲取神器。

這些工具用於執行以下活動：

- 建立後門能力
- 用於指揮和控制 (C&C)
- 竊取用戶憑證
- 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.NPPSpy!g2
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- 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。

2023/12/03

低成本的好意被來拿做壞事～駭客濫用Cloudflare R2物件儲存服務代管釣魚網頁的攻擊行動，散播Mars(*火星)竊密惡意程式

Mars 竊密惡意程式的破解版本非常普遍，而且不斷有新的駭客和個人取得這些版本，進而加劇全球範圍內持續存在的威脅。最近，一個攻擊者一直在使用相同的 Mars 竊密惡意程式二進位檔案發動各種惡意垃圾郵件活動，似乎沒有鎖定特定的目標受眾 (即全球所有組織都是潛在目標)。

在多數的回報案例中，電子郵件都包含一個惡意二進位附件 (Document.pif)。然而，在一次事件中，除了在電子郵件中附加惡意軟體外，他們還試圖透過轉向到架設在 CloudFlare R2 上的釣魚網站頁面的惡意連結來擷取使用者的電子郵件憑據 (請閱讀有關此釣魚策略的更多資訊--連結)。

觀察到的電子郵件主旨：

- 採購訂單號：4123001569
- 詢價單
- TRQ-983702]：您的 [收件人電子郵寄地址]電郵帳號服務即將到期

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：

- Trojan.Gen.MBT

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：

- System Infected: Trojan.Backdoor Activity 634

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。

2023/12/01

LEAKDB勒索軟體

『LEAKDB／也稱為 Phobos』是最近出現在真實網路情境的全新勒索軟體。它會加密用戶檔案，並冠上『.LEAKDB＋受害者 ID＋攻擊者的電子郵寄地址』副檔名。被成功加密後，勒索軟體會以文字檔：info.txt 的形式留下勒索 (贖金支付) 說明，要求受害者聯繫攻擊者，以獲取如何解密的進一步說明。

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：

- ACM.Untrst-RunSys!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Wbadmin!g1
- AGR.Terminate!g2
- SONAR.SuspDataRun

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Phobos!gm1

基於機器學習的防禦技術：

- Heur.AdvML.B

2023/12/01

糖衣往往是毒藥～SugarGh0st惡意軟體 ，其實是量身定制版本的Gh0st遠端存取木馬(RAT)

SugarGh0st 是源於 Gh0st 遠端存取木馬 (RAT) 家族的一個量身定制版本，已在真實網路情境出現。在針對烏茲別克外交部和韓國用戶的攻擊行動中檢測到它。感染鏈利用包含惡意 Javascript 的 Windows 捷徑檔來部署 DLL 載入器和執行 SugarGh0st 二進位檔案。該惡意軟體能夠收集系統詳細資訊、執行各種檔案操作、實現攻擊者的遠端控制、啟動反向 shell 以及執行攻擊者發送的任意命令。

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：

- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1
- ACM.Wscr-CPE!g1
- ACM.Wscr-CNPE!g1
- AGR.Terminate!g2
- AGR.Terminate!g6
- SONAR.SuspLaunch!g78

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Trojan Horse
- 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.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。

2023/11/30

Scarlet(*猩紅)惡意竊密程式

Scarlet 是另一個被大肆吹捧宣傳的竊取程式，二進位檔案在測試階段和真實惡意活動中都曾出現過。這種威脅與其他惡意竊密程式並無太大區別，因為它做的基本上是同一件事--竊取電腦資訊、網頁瀏覽器上的敏感性資料和加密貨幣錢包（包括 Exodus、Electrum、Atomic、Guarda、Coinomi、Monero、Ledger、Bitbox 和 Trezor）。它還透過 Telegram 機器人回報和外洩被盜資料。

會購買這種惡意竊密程式的駭客組織和個體戶，大部分還是用於竊奪一般消費者的加密貨幣錢包，但企業可能也不能倖免，因為它的其他竊取功能仍然構成嚴重的威脅。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Untrst-FlPst!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer

基於機器學習的防禦技術：

- Heur.AdvML.B!100

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 641