保安資訊--本周(台灣時間2024/05/03)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 51 萬 600 台受保護端點上總共阻止了 5,570 萬次攻擊。這些攻擊中有 82.8% 在感染階段前就被有效阻止：**(2024/04/29)**

- 在**11萬300**台端點上，阻止了**1,890萬**次嘗試掃描**Web**伺服器的漏洞。
- 在**14萬2,300**台端點上，阻止了**1,160萬**次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬6,700**台**Windows**伺服主機上，阻止了**920萬**次攻擊。
- 在**6萬7,500**台端點上，阻止了**190萬**次嘗試掃描伺服器漏洞。
- 在**1萬4,600**台端點上，阻止了**81萬8,100**次嘗試掃描在**CMS**漏洞。
- 在**4萬8,700**台端點上，阻止了**150萬**次嘗試利用的應用程式漏洞。
- 在**18萬6,100**台端點上，阻止了**420萬**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬1,300**台端點上，阻止了**150萬**次加密貨幣挖礦攻擊。
- 在**10萬7,400**台端點上，阻止了**810萬**台次向惡意軟體**C&C**連線的嘗試。
- 在**538**台端點上，阻止了**5萬6,500**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 15 萬 900 個受保護端點上阻止了總計 570 萬次攻擊。**(2024/04/29)**

- 使用網頁信譽情資，在 **136.8K** 個端點上阻止 **510** 萬次攻擊。
- 攔截 **30.9K** 個端點上 **543.6K** 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 **10.7K** 個端點上攔截 **99.5K** 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 **332** 個端點上攔截 **17.1K** 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。

2024/05/02
誰說老狗變不出新把戲？ZLoader變給你看！

ZLoader 是一隻模組化的金融木馬程式，早在 2007 年就已出現。最近發現其具有反分析的能力，這些能力似乎是從 ZeuS 原始程式碼中提取出來的。這種『新』的能力使 ZLoader 能夠阻止在初始感染發生的機器之外安裝，從而阻止進一步部署後續階段，進而阻礙深度分析。

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：

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.C

2024/05/02
Goldoon殭屍網路

根據 FortiGuard 實驗室最近一份報告，在真實網路情境觀察到一種名為 Goldoon 的全新殭屍網路。該惡意軟體利用 D-Link 2015 年的一個舊漏洞 (CVE-2015-2051) 進行傳播。Goldoon 可以在受影響的裝置上常駐，並執行從 C&C 伺服器接收到的命令。攻擊者可能會利用這種惡意軟體來控制受感染的裝置、收集系統資訊以及實施各種形式的分散式阻斷服務 (DDoS) 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 Horse
- 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。

2024/05/02

BirdyClient 惡意軟體濫用 Microsoft Graph API 進行 C&C 通訊

越來越多的威脅開始濫用微軟 Graph API，它的正面功能是可以存取 Office 365 中各種服務資料的 API，通常是為了進行與託管在微軟雲端服務上的命令與控制 (C&C) 基礎設施的通訊。這種技術最近被濫用於針對烏克蘭一個組織的攻擊，在這次攻擊中，一個名為 BirdyClient 的惡意軟體利用微軟 OneDrive 並使用 Graph API 實現 C&C 目的。

在我們的部落格文章中有更詳細的內容：Graph：利用 Microsoft API 的威脅數量正在增加。

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!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Graphican
- Backdoor.Graphon
- Trojan Horse
- Trojan.BirdyClient
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT
- WS.Malware.2
- VMware Carbon Black 產品中的現有政策已經阻止並檢測到相關的惡意指標。建議的最低策略是阻止所有類型的惡意軟體執行（已知、可疑和PUP），並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 信譽服務中獲得最大收益。

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
- Heur.AdvML.C

2024/04/29

DarkGate惡意程式載入器仍在大肆傳播

去年，DarkGate 惡意程式載入器的傳播非常氾濫。許多電子郵件攻擊行動利用各種攻擊鏈來傳播 DarkGate 有效酬載。據觀察，有的電子郵件包含直接下載連結，有的則可能使用附件 (PDF、ZIP 等) 來進行傳遞。

最近發現到一個攻擊行動初始階段是透過 XLSX 或 HTML 附件來傳遞 DarkGate。這兩種感染途徑都會透過 XLSX 中的巨集或 HTML 中的 Internet 捷徑檔下載下一階段的腳本。後續的腳本執行最終會衍生 DarkGate 惡意軟體有效酬載。

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
- ACM.Wscr-Ps!g1

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：

- Downloader
- ISB.Downloader!gen48
- ISB.Heuristic!gen107
- Phish.Html
- Scr.Malcode!gen136
- Trojan Horse
- Trojan.Darkgate

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。

2024/05/01

Dwphon手機／行動裝置惡意軟體

Dwphon 是最近發現一種針對安卓平臺的惡意軟體。該惡意軟體具有收集受感染裝置資訊、裝置上安裝的 APP 資訊以及一些機密個人資訊的功能。Dwphon 可能由幾個不同的模組組成，每個模組都有自己的功能和 C&C 指令。

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：

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

2024/05/01

金融木馬：SpyNote假冒哈薩克中央銀行為誘餌

沒有哪個國家或金融機構能倖免於其品牌被冒用來誘使手機／行動裝置使用者安裝安卓惡意軟體的命運--這種趨勢還在繼續增長。賽門鐵克最近觀察到一名威脅者，正利用知名的金融木馬：SpyNoteSpyNote 積極瞄準哈薩克的用戶。

為了取得受害者的信任，威脅者將其 APP 命名為『 "Поддержка национального банка Kz.apk』(翻譯為『支持哈薩克國家銀行』)，這顯示他們正在利用哈薩克中央銀行作為誘餌。目前還不清楚該惡意程式是如何傳播，但很可能是透過惡意簡訊，也可能是透過不同 APP 啟動。

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：

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

2024/04/30

GuLoader惡意軟體下載器，涉入針對俄語系國家的網路攻擊

已觀察到一名威脅者利用不同的社交工程手法發動兩起電子郵件攻擊行動，這些行動都有 Guloader 涉入的跡象。這兩起電子郵件攻擊行動都針對俄語系國家，例如：俄羅斯、白俄羅斯、吉爾吉斯和哈薩克的產業。

在一封電子郵件 (主旨：СПЦ №130 подписанная Belarus) 中，他們冒充一家從事製藥和保健行業的俄羅斯大型公司。該公司有多個業務部門，包括藥品行銷、零售連鎖藥店和醫藥產品製造。攻擊者使用類似銷售的社交工程手法，夾帶一個壓縮附件檔 (СПЦ №130 от 12.04.2024 подпис.7z)，並誘使受害者執行其中偽裝成產品特性摘要的惡意二進位檔案 (СПЦ №130 от 12.04.2024 подпис..exe)。

在分析上述攻擊情境時，賽門鐵克在公開來源中發現另一個惡意壓縮檔 (Доверенность Транзит Хоргос.7z)，其中包含完全相同的 GuLoader 有效酬載。因此，作者似乎也在使用不同的電子郵件方案開展並行活動 (儘管目前還無法獲得該電子郵件)。根據其名稱，威脅者試圖用與霍爾果斯貨物過境相關的法律檔案引誘受害者。霍爾果斯是哈薩克和中國邊境上的一個重要地點，因其作為主要陸港和新絲綢之路經濟帶上的樞紐而聞名，促進中國、中亞和歐洲之間的大量貿易和物流業務。

GuLoader 是一種惡名昭章的惡意軟體下載器，因其經常涉入世界各地的攻擊行動被用於傳播各種惡意軟體而聞名。在本案例中，它正在載入 Agent Tesla 惡意竊密程式，但也可能下載 Remcos 遠端存取木馬。

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)。

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：

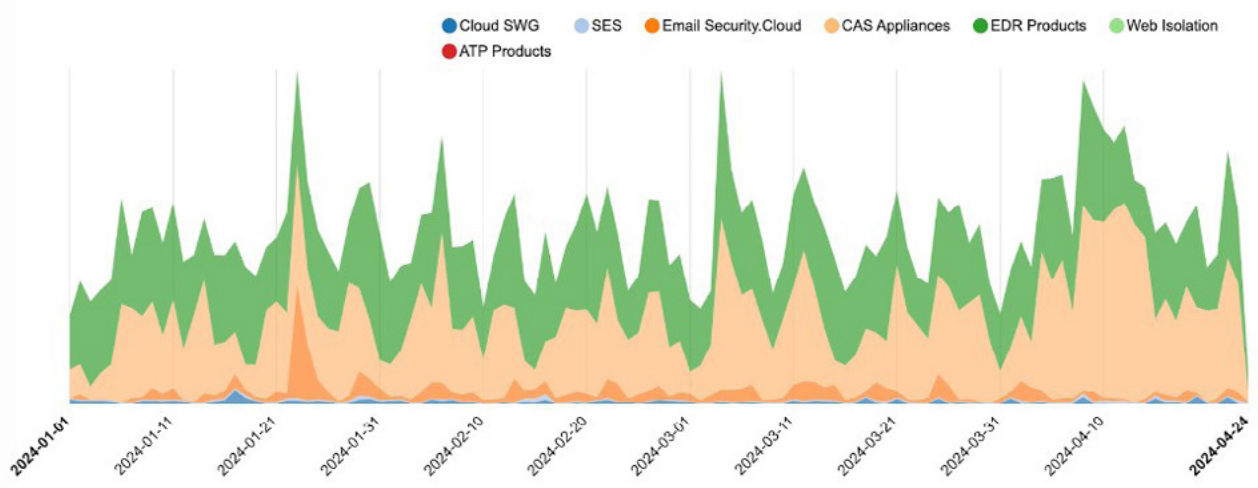
- Trojan Horse

2024/04/30
防護亮點：賽門鐵克雲端沙箱--提供全新和未知威脅的進階防護

在不斷變化的威脅環境中，惡意威脅者不斷提高其人力與資源，以產出精密又複雜的全新惡意軟體。所幸賽門鐵克雲端沙箱提供一個深入分析惡意軟體的領先平臺，以確保既能適當地檢測到這些日新月異的惡意軟體，又能提供足夠的中繼資料來幫助威脅獵捕和關聯能力。數十年來，賽門鐵克一直致力於構建快速、精準以及大規模識別惡意檔案的技術，透過賽門鐵克雲端沙箱，我們可直接為您的組織提供賽門鐵克的完整分析能力。

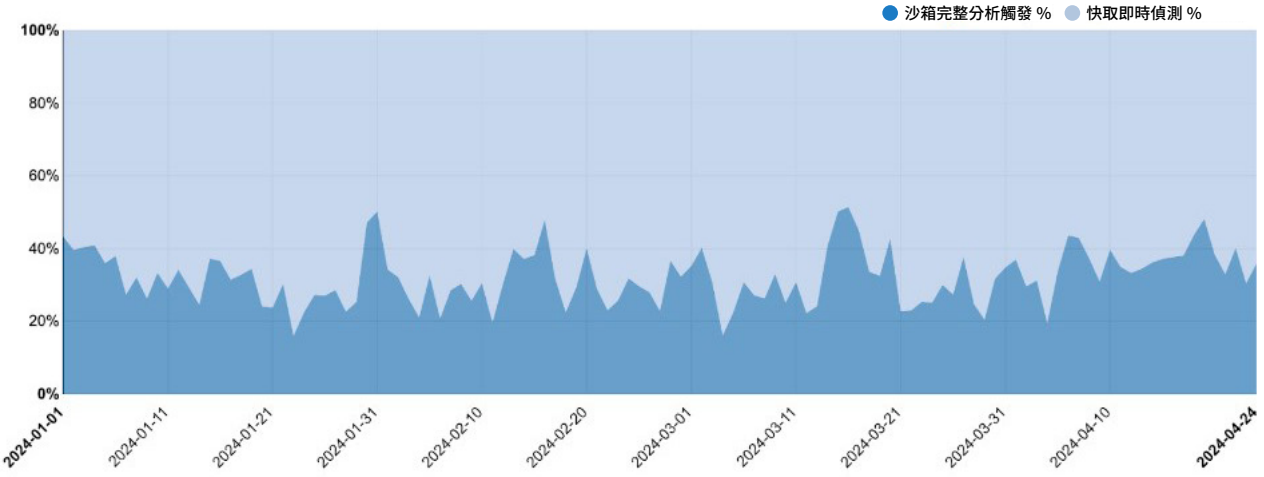
受益於雲端架構的即時性與擴充延展優勢，賽門鐵克雲端沙箱可為賽門鐵克安全產品組合中的內部部署和基於雲的安全產品提供雲端託管分析功能。除了提供行為分析的標準沙箱外，賽門鐵克雲端沙箱也提供端點或正常雲端分析安全產品所不具備的尖端檢測技術和功能。

數字會說話：賽門鐵克雲端沙箱為各種產品組合提供的保護成績單



雲端沙箱處理的流量在設計上明顯小於整體產品流量，因為每個產品都有完整的多層次保護技術，只有其他技術檢測不到的檔案才會被過濾到雲端沙箱。這凸顯單個產品的多層次保護技術，在應對絕大多數威脅時的出色表現。對於郵件安全雲端服務：Email Security Cloud和網頁安全雲端服務：CloudSWG 等產品而言，某些威脅的發展速度足以在短時間內繞過靜態掃描技術--在這種情況下，賽門鐵克雲端沙箱會進行分析並為客戶提供保護。這裡的檢測結果也會與我們的全球威脅情資網路 (GIN) 共享，提供即時回饋，同步提升其他賽門鐵克產品和服務的整體安全態勢，進而大大提升客戶體驗。

為解決方案提供最即時的攔截能力



在賽門鐵克雲端沙箱所有檢測中，有 60% 以上檢測結果都是早已提交過的惡意軟體。一旦新增的檢測結果從沙箱即時更新到快取，該解決方案就可提供即時攔截，無須經由沙箱引爆。

賽門鐵克雲端沙箱的主要功能

- 提供三種資料留存位置選項 (美國、歐洲和全球)，允許客戶選擇惡意軟體引爆地點。
- 使用賽門鐵克全球威脅情資網路審查檔案的中繼資料，消除已知威脅和良性流量。
- 利用檔案內容、出現時間、頻率和其他因素來識別可能被遺漏的威脅。

- 透過進階機器學習，檢測已知威脅和不斷演變的威脅。
- 靜態分析採用靜態掃描、反解譯、統計／熵分析、模擬和多層次嵌入／編碼的 artifact extraction 等方法。
- 惡意軟體的執行是在受控沙箱環境中進行，在這種環境中，有人的存在感和隨機化等技術允許惡意軟體暴露自己並展示所有可能的特徵，以便正確識別。
- 大量新的尖端威脅防護技術透過僅在雲平臺上提供的額外資源套用於樣本。
- 賽門鐵克網頁 (URL) 分類服務依靠全球威脅情資網路來識別威脅、威脅產出物和惡意網路活動。
- 除了引爆後的行為、網路和產出品分析外，賽門鐵克雲端沙箱並在引爆期間對樣本進行主動線上評估，進而提供更豐富的情境感知惡意軟體分析。

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。
欲瞭解有關 Symantec 端點偵測與回應 (EDR) 最新簡報檔，請點擊此處。

2024/04/29

發現DragonForce勒索軟體新變種

據觀察，一種名為 DragonForce 的勒索軟體新變種是使用 LockBit 勒索軟體組織遭洩露的勒索軟體產生器所產出。

DragonForce 勒索軟體以勒索受害者為目標。威脅者通常會採用雙重勒索戰術，讓受害者無法存取遭感染的電腦以外，並在加密前滲出資料。如果受害者無法乖乖就範付贖金，威脅者就會在暗網公開發佈受害者的資料。

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

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransom!gen82
- SONAR.TCP!gen1
- SONAR.UACBypass!gen30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Lockbit!g6
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.2
- WS.SecurityRisk.4

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

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: Bad Reputation Application Network Activity

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。

2024/04/29

近期假冒資安軟體的網路攻擊行動

冒充合法應用程式是攻擊行動中常見的戰術。其中最簡單的冒充方法是利用合法的檔案名稱說服受害者執行該程式。Sophos 最近發佈一份報告中指出，攻擊者正在修改資安軟體廠商的合法二進位檔案，以啟動新嵌入的惡意酬荷。值得注意的是，修改此類檔案會破壞數位簽章，反過來也會降低應用程式的合法性。

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-Wscr!g1
- ACM.Rgasm-Lnch!g1
- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1
- ACM.Wmip-Net!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Dropper
- SONAR.Stealer!gen1
- SONAR.SuspBeh!gen6
- SONAR.SuspBeh.C!gen1
- SONAR.SuspLaunch!g405
- SONAR.SuspLaunch!g406
- SONAR.SuspProfileRun
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Cobalt!gm1
- ISB.Downloader!gen195
- Scr.Malcode!gen137
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.IcedID
- Trojan.Latrodectus
- Trojan.Pikabot
- Trojan.Pikabot!gen11
- Trojan.Pikabot!gen13
- WS.Malware.1
- WS.SecurityRisk.4

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
- 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。

2024/04/29

免費的永遠最貴～Ziraat惡意竊密程式偽裝成資料復原工具

發現一種偽裝成資料復原工具的基於 .NET的Ziraat 惡意竊密程式。該惡意軟體能夠從瀏覽器、社交媒體平臺和各種電子郵件應用程式中擷取密碼和憑證。此外，它還能進行螢幕截圖和鍵盤側錄。該惡意軟體被歸類為專門的遠端存取木馬 (RAT)，能夠從遭入侵的系統中擷取敏感資訊。

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-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1

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.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/04/29

利用MSIX安裝程式和惡意廣告來散播FakeBat惡意軟體的網路攻擊行動呈上升趨勢

最近有多起 FakeBat 惡意軟體涉入的網路攻擊行動，並有不斷增加的趨勢。FakeBat 利用多種傳播途徑，其中惡意廣告是主要手法。利用包括谷歌廣告在內的線上廣告平臺來傳播惡意軟體。FakeBat 獨特之處在於，威脅者使用 MSIX 安裝程式，並將其與嚴重混淆的 PowerShell 程式碼打包在一起。

在最近觀察到一次行動中，用戶被一個包含混淆 PowerShell 腳本的 Trello MSIX 軟體安裝程式所引誘。該腳本與命令與控制 (C&C) 伺服器通訊，以聽命下載後續階段的有效酬荷。這些有效酬載通常包括 SectopRAT 或 ArechClient2，並使用 IDAT 載入器技術將其注入 MSBuild 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.Rgasm-Lnch!g1
- ACM.Ps-Rd32!g1

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.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/04/26

中繼資料管理平臺OpenMetadata存在多個漏洞

OpenMetadata 是一個開源中繼資料平臺，可用於資料探查、資料型錄和協作。根據最近的一份報告，威脅者一直在利用 OpenMetadata 中的關鍵漏洞，包括身份驗證繞過和 Spring 表達式語言 (Spring Expression Language，SpEL) 注入攻擊，進而導致挖礦劫持軟體的部署。最近披露的 OpenMetadata 漏洞包括 CVE-2024-28253、CVE-2024-28254、CVE-2024-28255、CVE-2024-28847 和 CVE-2024-28848，影響 1.3.1 之前的版本。如果被成功開採濫用，所討論的漏洞可能允許未經認證的遠端攻擊者在受影響的實例上實現遠端程式碼執行 (RCE)。

賽門鐵克的網路保護技術入侵預防系統 (IPS) 會阻止這些漏洞利用嘗試，以防止系統遭受進一步感染／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：

- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.NPE
- SMG.Heur!gen

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: Malicious Java Payload Upload 2
- Web Attack: Malicious Java Payload Upload 22
- Web Attack: OpenMetadata Auth Bypass Vulnerability CVE-2024-28255

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。

2024/04/26

KageNoHitobito勒索軟體

KageNoHitobito 勒索軟體於 2024 年 3 月出現。這是一款簡單陽春的勒索軟體，具有基本的過時功能：檔案加密 (僅在本機磁碟機上)、留下贖金支付說明，並要求透過 Tor 交密會話與攻擊組織進行互動。沒有跡象顯示該勒索軟體具有竊取資料進行勒索的功能。資料顯示，該勒索軟體已在全球多個國家出現。

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：

- Ransom.Zombie
- 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