保安資訊--今日最新(台灣時間2024/04/26)
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 4,800 台受保護端點上總共阻止了 5,580 萬次攻擊。這些攻擊中有 82.9% 在感染階段前就被有效阻止：**(2024/04/22)**

- 在**10**萬**6,200**台端點上，阻止了**1,920**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13**萬**9,000**台端點上，阻止了**1,090**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3**萬**6,200**台**Windows**伺服主機上，阻止了**920**萬次攻擊。
- 在**6**萬**6,500**台端點上，阻止了**210**萬次嘗試掃描伺服器漏洞。
- 在**1**萬**3,600**台端點上，阻止了**81**萬**7,800**次嘗試掃描在**CMS**漏洞。
- 在**4**萬**9,000**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**19**萬**300**台端點上，阻止了**430**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1**萬**5,600**台端點上，阻止了**160**萬次加密貨幣挖礦攻擊。
- 在**10**萬**9,000**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**540**台端點上，阻止了**5**萬**8,100**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 15 萬 1,800 個受保護端點上阻止了總計 580 萬次攻擊。**(2024/04/22)**

- 使用網頁信譽情資，在 **137.2K** 個端點上阻止 **510** 萬次攻擊。
- 攔截 **31.6K** 個端點上 **557.8K** 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 **11.4K** 個端點上攔截 **109.6K** 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 **406** 個端點上攔截 **23.5K** 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。

點擊此處獲取--關於賽門鐵克原廠防護週報

2024/04/25

Brokewell：手機／行動裝置平台上的全新惡意軟體

在真實網路情境發現手機／行動裝置平台上的全新惡意軟體：Brokewell 。根據最近一份報導，該惡意軟體透過偽造成谷哥 Chrome 瀏覽器更新安裝套件傳送給安卓平台的用戶。該惡意軟體具有多數惡意竊密程式的功能，包括硬體資訊收集、憑證外滲、通話記錄檢索、音訊擷取、螢幕串流分享、點擊側錄、滑動和文字輸入以及其他各種遠端存取和裝置接管功能。

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：

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

2024/04/25

Amadey(*阿馬代)惡意軟體家族仍然活躍在威脅生態圈

Amadey 是一種以多元附加功能而聞名的惡意竊密程式，可下載和執行勒索軟體等惡意有效酬荷。雖然這個惡意軟體家族已經存在較長的時間，但幾乎每天都會在真實網路情境發現新的後繼新版本。模組化的架構與資訊竊取和有效酬載載入器的功能相結合，使該惡意軟體被不同的駭客組織用於各種攻擊行動中。據瞭解，Amadey 的傳播途徑包羅萬象，包括惡意附件、偽裝成破解版軟體的偷渡式下載、惡意廣告或漏洞利用工具包。

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：

- AGR.Terminate!g2
- SONAR.MalTraffic!gen1
- SONAR.SuspBeh!gen616
- SONAR.TCP!gen1
- SONAR.UACBypass!gen30

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Amadey
- Trojan.Amadey!g1
- Trojan Horse
- Trojan.Gen.2
- 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

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: Activity - Bad Application Reputation Application 7
- System Infected: Bad Reputation Process Request 4
- 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。

2024/04/24

濫用被動過手腳的『聯絡表單』網路攻擊行動中，SSLoad和Cobalt Strike涉入其中

一種名為 SSLoad 的全新惡意軟體載入器出現了，它與已知的 SLoad 截然不同。報告顯示，攻擊者透過聯絡表單濫用和發送惡意連結。點擊這些連結會下載並安裝 SSLoad 惡意軟體，然後這個基於 DLL 的惡意軟體載入器會部署更多後門和有效酬載，包括一個 Cobalt Strike 的信標，用於與攻擊者的 C&C 伺服器建立連接，以竊取系統和使用者資訊。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen195
- PUA.Gen.2
- Scr.Malcode!gen137

- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.3
- WS.SecurityRisk.4
- W32.Fixflo.B!inf

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

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: Scripting Host Processes Making Network Connections
- 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。

2024/04/24

SpyNote被涉入以越南國家公共服務局為誘餌的網路攻擊行動中

手機上的遠端存取木馬：SpyNote 及其後繼新變種正在全球各地大肆擴散，一些駭客組織和個體戶利用各種社交工程手法瞄準手機／行動裝置的使用者。在最近一次攻擊行動中，賽門鐵克發現該威脅 (DEDAWCH VCONG.apk) 偽裝成越南的國家公共服務門戶網站的官方 APP，該平臺為公民和企業提供廣泛的線上公共服務。

此一特定行動在越南造成嚴重影響，也在加拿大和波蘭等其他國家出現過。目前，還不清楚這款惡意程式是如何傳播的。

SpyNote 允許壞人遠端控制受感染的安卓手機／行動裝置，能夠存取和竊取敏感性資料、監控用戶活動，甚至在使用者不知情的情況下啟動鏡頭和麥克風等硬體來盜錄裝置上的影像與音訊等。

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：

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

2024/04/24

APT43駭客組織利用Dropbox雲端硬碟來散播TutorialRAT惡意程式的網路攻擊行動

APT43 駭客組織被發現利用 Dropbox 雲端硬碟積極傳播 TutorialRAT 惡意程式，以此作為其攻擊的基地，以規避資安威脅監控。該行動似乎是 APT43 駭客組織已發動的 BabyShark 攻擊行動的延伸，並採用典型的魚叉式網路釣魚技倆，包括使用捷徑 (LNK) 檔。TutorialRAT 是一個基於 C# 的遠端控制程式，具有資訊竊取功能，可收集和滲出裝置和使用者的個人資訊。

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.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g20
- SONAR.Powershell!gen5

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen10
- ISB.Downloader!gen175
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- 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: Dropbox Cloud Service Connect Attempt
- Audit: Powershell Process Accessing Dropbox API Activity

2024/04/24

駭客組織：CoralRaider傳播新版CryptBot惡意竊密程式的網路攻擊行動

根據最近的一份報告，在同時散播三種不同的惡意竊密程式 Cryptbot、LummaC2 和 Rhadamanthys 的網路攻擊行動中，這些惡意竊密程式歸屬於駭客組織：CoralRaider 所有。威脅者一直在利用「內容傳遞網路」(CDN：Content Delivery Network) 的快取作為惡意軟體的傳遞機制。CryptBot 惡意軟體的新變種具有從遭入侵電腦中竊取各種資料的功能。它的目標是從網頁瀏覽器、加密貨幣錢包、身份驗驗證和密碼管理應用程式中滲出資料。

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.Mshta-Cmd!g1
- ACM.Mshta-Http!g1
- ACM.Mshta-Ps!g1
- ACM.Ps-Http!g2
- ACM.Ps-Reg!g1
- ACM.Ps-Mshta!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen1
- SONAR.SuspScript!g7
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen55
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1
- 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!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: 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。

2024/04/24

駭客組織：Seedworm利用Atera Agent安裝程式，發動魚叉式網路釣魚

駭客組織：Seedworm (也被稱為 MuddyWater) 正在大肆利用合法的遠端監控和管理 (RMM) 工具 Atera Agent 進行其魚叉式網路釣魚行動。攻擊者利用 Atera 提供的 30 天免費試用服務，建立註冊在已遭入侵的電子郵件帳戶上的代理，進而不用自己建立命令與控制 (C&C) 基礎設施的情況下遠端存取目標系統。Atera 透過其網頁式操作介面提供廣泛的遠端控制功能，包括檔案上傳／下載、互動式 shell 存取和人工智慧輔助命令。攻擊者利用免費的檔案託管平臺上架其 RMM 安裝程式，並透過魚叉式網路釣魚郵件進行傳播。

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.Malmsi
- WS.Malware.1

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: Atera Client 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。

2024/04/23

誤安裝假冒求職APP，石油產業的求職者的簡訊遭劫持

賽門鐵克最近觀察到一個惡意攻擊行動以鎖定在石油產業的求職者。他們製作一個假冒的求職 APP 安裝套件 ([公司名稱] Jobs.apk)，像極了是出自巴林和中東的知名石油產業企業。不疑有它被誘騙安裝該 APP 的使用者會被引導在一個表格中輸入手機電話號碼。使用者並不知道，惡意程式實際上會監控並攔截竊取所有的簡訊內容。

惡意行為者出於各種邪惡目的收集受害者的簡訊。包括攔截雙因子驗證碼以未經授權的瀏覽個人和金融帳戶、利用一次性密碼等敏感資訊進行金融詐騙、竊取個人資訊進行身份盜竊、收集聯絡資訊以進一步實施更精準網路釣魚計畫，以及可能進行企業間諜活動，特別是在石油等經常交換敏感資訊的行業。

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。

- AppRisk:Generisk

2024/04/23

安卓平台上充斥者日益增多的假冒MetaMask APP，覬覦使用者的加密貨幣錢包

安卓平台上假冒的 MetaMask APP 日益增多，多是透過網路釣魚伎倆瞄準手機／行動裝置用戶的加密貨幣錢包，這些假冒的 APP 都上架在假冒的 MetaMask 網站並利用誤植網域或打錯字的錯誤。很可能這些 APP 是透過惡意簡訊傳播的。

此一增長趨勢主要是因為 MetaMask 是一個廣受歡迎的加密貨幣錢包，也是乙太坊區塊鏈上去中心化應用 (dApps) 的入口。它的受歡迎使其成為攻擊者利用其聲譽和用戶群體謀取財務利益的主要目標。

雖然一般個人是 MetaMask 的主要使用者，但在某些情況下，企業或商業機構也會出於特定目的使用某些功能或與之整合，例如：管理加密貨幣資產或與基於區塊鏈的系統進行互動。不過，MetaMask 的主要關注點和用戶群是個人消費者。

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：

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。

- 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。

2024/04/23

防護亮點：下載鑑識--基於檔案信譽的零時差保護技術

不受信任的檔案下載正為各種線上威脅敞開大門。惡意軟體、勒索軟體，甚至複雜的網路

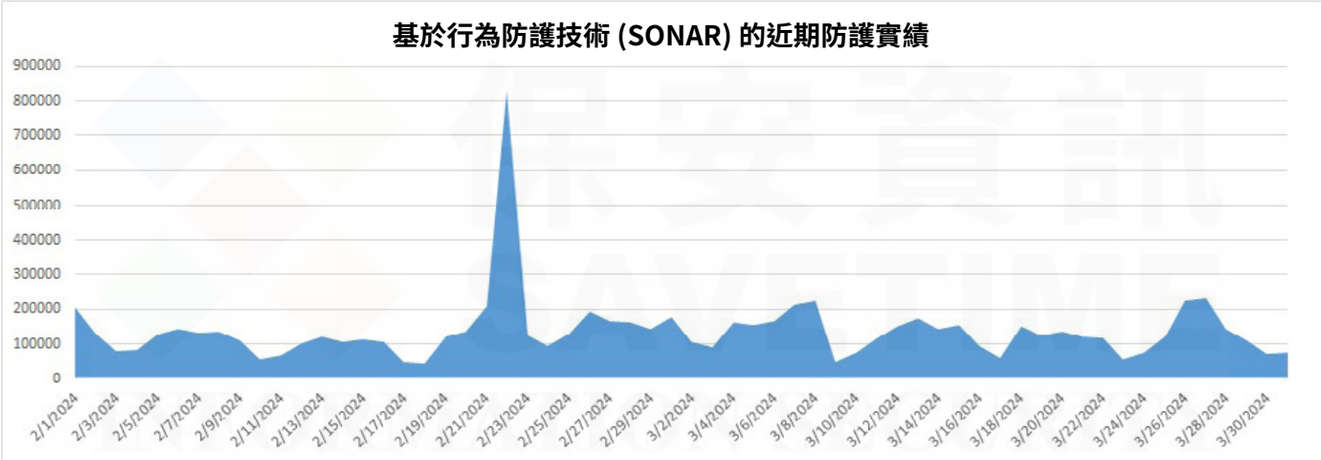
攻擊都只需透過單一個受感染的檔案滲入您的網路。一旦進入系統，這些威脅就會造成嚴重破壞、竊取敏感性資料、干擾運營並導致財務損失。「多元的入口」就是典型的感染與入侵的媒介--諸如瀏覽器、下載器、網路聊天程式和壓縮軟體等應用程式，這些都是檔案進入系統的門戶。就像一名守衛站在您家門外一樣，**賽門鐵克下載鑑識 (Symantec Download Insight)** 即時監視多個門戶，確保下載檔案的安全性。

賽門鐵克下載鑑識 (Symantec Download Insight) 的獨特之處在於，它能夠利用賽門鐵克檔案信譽來防範千奇百怪的威脅。賽門鐵克檔案信譽不僅能識別威脅，還能瞭解全球威脅環境中每個檔案的來龍去脈。當檔案與諸如不良用戶--機器行為、最近使用時間、低普及率、不受信任的數位簽章、不受信任的來源以及數百個其他聲譽不佳指標相關聯時，就會被評為可疑的檔案。將這些聲譽不佳最明顯指標與該檔案是透過各種入口下載這一事實相結合，就會被攔截。

賽門鐵克檔案信譽包括超過 90 億個檔案的信譽，並根據來自數百萬個端點即時遙測大數據、多個威脅來源和賽門鐵克安全回應分析師專業團隊的專家分析進行持續更新。

行為攔截--利用行為引擎和檔案信譽提供零時差保護

賽門鐵克檔案信譽也可與賽門鐵克行為防護引擎 (稱為 SONAR) 構成聯防機制。SONAR 可追蹤可疑的程序行為，例如：下載程式、篡改、勒索軟體行為等，並使用賽門鐵克檔案信譽來證實這些可疑行為的不良信譽。



利用 SONAR 和檔案信譽 (File Reputation) 主動攔截全新威脅的實例包括：

- 勒索軟體
- Conti
- Quasar
- Sality
- Emotet
- Qakbot
- Trickbot
- Mimikatz
- Wannacry

欲深入瞭解下載防護：下載鑑識 (Download Insight) 更多資訊，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 如何使用 Symantec Insight 進行檔案相關決策，請點擊此處。
欲深入瞭解何謂賽門鐵克行中的行為分析 (SONAR)？請點擊此處。

2024/04/23

GooseEgg(*鵝蛋)～專用於後攻擊的惡意軟體

Microsofthave 的研究人員報告賽門鐵克識別為 Swallowtail(又名 STRONTIUM) 的俄羅斯駭客組織：Forest Blizzard 利用名為 GooseEgg 的定制行惡意工具正在進行的活動。此活動至少從 2020 年就開始，最早可能在 2019 年。該惡意軟體濫用 WindowsPrint Spooler 服務中的一個漏洞 (CVE-2022-38028) 來獲得系統層級的權限，並從遭入侵的網路中竊取憑證。最近觀察到的網路攻擊行動主要針對烏克蘭、西歐和北美的政府、非政府、教育和運輸部門組織。

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：

- Trojan.GooseEgg
- Trojan Horse
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/04/22

Kapeka後門程式

Kapeka 後門程式涉入最近針對東歐各個組織機構的惡意攻擊行動，該後門程式至少自 2022 年以來一直遭濫用。據信這個後門是由知名 Sandworm 的駭客組織所傳播。Kapeka 後門是採 C++ 撰寫，具有對受害者機器指紋辨識、執行shell命令、讀寫檔案的能力或啟動任意有效籌載等功能。Kapeka 還具有升級後門二進位檔案或從受感染的端點完全自我刪除之功能。

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：

自適應防護技術(包含於SESC)：

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

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：

- Trojan.Kapeka
- 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。

2024/04/22

Sharpil遠端存取木馬(RAT)--可能是Sharp惡意竊密程式的前身

Sharpil 是在威脅環境中發現一種新的遠端存取木馬 (RAT)。這種採用 C# 語言撰寫的惡意軟體具有基本資訊竊取功能，包括系統資訊收集和從各種網路瀏覽器中收集資料。一旦入侵受感染的電腦，Sharpil 會透過 Telegram 機器人與攻擊者建立連線。Sharpil 與另一種最近發現的惡意軟體 Sharp 惡意竊密程式的程式碼有些雷同之處。與 Sharpil 相比，據報導這個變種在 Telegram 上被宣傳出售，並且功能上具有一些增強能力。

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

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.A!400
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- 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: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 568

2024/04/21

Core Werewolf進階持續威脅(APT)駭客集團發動的間諜行動以俄羅斯國防組織為目標

Core Werewolf 進階持續威脅 (APT) 駭客集團的間諜活動瞄準俄羅斯的國防機構，大約在四月中旬被觀察到。這次攻擊利用一個惡意檔案作為誘餌，據稱是為了向特種部隊士兵頒發國家獎章。然而，該檔案實際上是一個 7zSFX 的壓縮檔，內含一個合法的遠端存取工具 UltraVNC。在解壓縮後，惡意軟體會產生誘餌檔案和 UltraVNC 可執行檔的副本，進行可執行檔的排程任務，並與指定伺服器建立連接。

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-Schtsk!g1

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.MBT
- WS.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2024/04/21
Megazord勒索軟體

Megazord 勒索軟體是由 Rust 程式語言所撰寫，主要鎖定醫療保健、教育和政府機構。初始攻擊的途徑包括針對特定目標的釣魚郵件以及開採濫用易受攻擊的服務。RDP 和進階 IP 掃描器等工具被用於橫向移動。一旦遭入侵，Megazord 將終止多個程序和服務，並加密本機磁碟和檔案。被加密的檔案會被冠上『.POWERRANGES』的副檔名，並在被加密檔案所在的資料夾中放置勒索贖金支付說明檔『powerranges.txt』。受害者被指示透過 TOX 加密訊息與加害者聯繫，並按照勒索贖金支付說明中提供的唯一 Telegram 頻道連結。Megazord 的程式碼與 Akira 有許多雷同之處，據信與 Akira 勒索軟體有所關聯。

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.Akira!g2
- Trojan.Gen.MBT
- W97M.Downloader
- 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

2024/04/21
藏身在.DOC檔案的OfflRouter惡意程式正在危害烏克蘭

威脅研究人員最近在真實網路情境觀察到的各種 . DOC 檔案中內藏 OfflRouter 病毒。這些檔案包含 VBA 程式碼，一旦被開啟就會下載一個可執行檔，該檔會開始在機器上尋找其他 DOC 檔案進行感染，並在抽取式儲存裝置上搜索其他外掛程式。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen
- W97M.Downloader

基於機器學習的防禦技術：

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

2024/04/19
Coreid(又稱Fin7)駭客集團利用惡意後門程式攻擊美國汽車製造商

最近報告提供 Coreid(又稱Fin7) 駭客集團鎖定美國汽車製造業的網路攻擊活動詳情。報告稱，該行動利用魚叉式網路釣魚電子郵件，透過免費線上掃描工具相關的社交工程內容對鎖定的目標進行攻擊。受害者會被誘騙點擊一個連結，進入一個假的線上掃描相關網站。由此展開攻擊鏈後續將會下載負責部署最終後門有效酬載的多階段元件。

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.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Dropper
- 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

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。

2024/04/19

進階持續威脅(APT)駭客集團利用Web3遊戲熱潮進行加密貨幣竊取的行動

觀察到一個以模仿 web3 這種建立在區塊鏈和去中心化科技基礎上遊戲形式的網路攻擊行動，可能是由一個以俄語為主要語言的進階持續威脅 (APT) 駭客集團所運營，其目的在利用基於區塊鏈的遊戲的吸引力，透過獲取潛在的加密貨幣收益。用戶被誘使訪問這些遊戲的主要網頁以下載軟體。一旦安裝，該軟體會進一步感染設備，安裝惡意竊密程式。根據作業系統的不同，惡意軟體變種包括 Atomic macOS Stealer (AMOS)、Stealc、Rhadamanthys 或 RisePro。

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：

- OSX.Trojan.Gen
- 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。

2024/04/19

Akira勒索軟體在威脅環境中仍是一個活躍的威脅

賽門鐵克安全回應中心 (Symantec Security Response) 瞭解到 CISA、FBI、歐洲刑警組織歐洲網路犯罪中心 (EC3) 和荷蘭國家網路安全中心 (NCSC-NL)，最近都觀察到 Akira 勒索軟體涉入的活動並聯合發出警報。Akira 至少從 2023 年起就出現在威脅環境中的勒索軟體家族。根據已發佈的報告，『Akira』仍是一個活躍的威脅，迄今已涉入攻擊 250 多個組織。Akira 加密勒索軟體最初的版本是採用 C++ 所撰寫，被其加密後的檔案會被冠上 .akira 副檔名。去年出現的後繼新變種

Megazord 則是改用 Rust 語言所撰寫，被其加密後的檔案會被冠上 .powerranges 副檔名。Akira 除了有 Windows 平台的版本，該勒索軟體幕後的組織還發佈 Linux 平台的版本，主要鎖定 VMware ESXi 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.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g138
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Akira
- Ransom.Akira!g2
- 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
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.C

2024/04/19

針對 iOS 裝置的 XAgent 間諜軟體

一款針對 iOS 裝置的 XAgent 間諜軟體已經被證實與 Swallowtail 駭客集團 (APT28) 有所關連。XAgent 主要針對西歐的政治和政府機構，具有遠端控制和資料滲透功能。它可以收集使用者的連絡人、資訊、裝置詳情、已安裝的 APP、螢幕截圖和通話記錄等資訊。這些資料有可能被用於社交工程或魚叉式網路釣魚行動。

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.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。

2024/04/19

透過假冒網站傳播MadMxShell後門的惡意軟體行動

被稱為 MadMxShell 的全新後門程式涉入惡意軟體攻擊行動。發動該網路攻擊行動的歹徒，建立一個假冒合法 IP 掃描軟體下載的網站。他們利用網址誤植錯誤、購買搜尋引擎排名等伎倆，透過谷歌廣告吸引用戶。該後門利用 DNS MX 查詢進行命令和控制 (C&C) 通訊，目的在躲避記憶體取證安全解決方案。該惡意軟體為攻擊者提供對受損系統的未經授權存取，使他們能夠執行命令、外洩資料並進行其他惡意活動。

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-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.B!100

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。