保安資訊--本周(台灣時間2024/04/19)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 49 萬 3,700 台受保護端點上總共阻止了 5,600 萬次攻擊。這些攻擊中有 84.8% 在感染階段前就被有效阻止：**(2024/04/15)**

- 在**10萬3,300**台端點上，阻止了**2,020**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**12萬7,400**台端點上，阻止了**950**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,500**台**Windows**伺服主機上，阻止了**9,00**萬次攻擊。
- 在**6萬4,500**台端點上，阻止了**230**萬次嘗試掃描伺服器漏洞。
- 在**1萬7,000**台端點上，阻止了**100**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬5,700**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**17萬9,400**台端點上，阻止了**450**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬6,000**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**10萬6,200**台端點上，阻止了**720**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**440**台端點上，阻止了**4萬6,800**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 13 萬 9,800 個受保護端點上阻止了總計 550 萬次攻擊。**(2024/04/15)**

- 使用網頁信譽情資，在 **126.8K** 個端點上阻止 **490** 萬次攻擊。
- 攔截 **28.7K** 個端點上 **546.6K** 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 **10.3K** 個端點上攔截 **105.3K** 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 **408** 個端點上攔截 **19.2K** 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。

2024/04/18

CR4T惡意軟體植入程式在DuneQuixote網路攻擊行動中大肆散播

據報導，名為 DuneQuixote 網路攻擊行動中傳播 CR4T 惡意軟體植入程式的後繼新版本。該行動目標是中東地區的各種組織和機構。CR4T 惡意軟體有兩種不同的版本，一種用 C/C++ 撰寫，另一種用 Golang 程式設計語言撰寫。該惡意軟體的功能主要是允許攻擊者存取受感染的端點，實現遠端命令執行和任意檔案的上傳／下載功能。

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.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 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

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。

2024/04/18

Mamont：安卓平台上的銀行金融木馬

Mamont 是最近發現安卓平台上的銀行金融木馬。該惡意軟體偽裝成谷歌瀏覽器的安裝套件檔散佈。Mamont 具有收集受感染裝置資訊的功能。它可以擷取選定的訊息並攔截新訊息，並將其轉發送回攻擊者控制的 Telegram 頻道。該惡意軟體有能力檢查訊息內容，特別關注的是與任何金融或貨幣交易相關的訊息。

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

2024/04/17

Google建置Web與行動應用程式的後端平台：Firebase和知名潛在客戶開發系統：Clearbit成為網路釣魚行動的幫兇

網路釣客的手法多如牛毛，從雲端服務到社交工程，使其騙術更具說服力。在雲端服務中，谷歌的 Firebase 因其易用性、免費、可擴展性和網域定制功能而被廣泛濫用。這些特性使其成為一個吸引網路釣客的平臺，他們只需花費最少的精力和成本就能上架和傳播詐騙內容。

在社交工程手法上，網路釣客越來越熟於使用電子郵件地址的查詢字串動態生成網路釣魚頁面。為了進一步增加可信度，他們一直在利用 Clearbit(logo.clearbit.com)，根據受害者的電子郵件地址網域查找該公司的 logo，然後將其顯示在網路釣魚頁面上。透過利用合法 logo，網路釣客可以顯著提高上鉤率，進而可能給目標公司造成經濟損失、資料洩露和信譽損害。

舉例說明最近看到與上述手法相關的釣魚網頁的網址：

- hxxps://firebasestorage[.]googleapis[.]com/v0/b/fficeme-a6187[.]appspot[.]com/o/jyps%2Fauth%2FLogin[.]html?alt=media&token=5e00a67b-5b1a-4cc9-85cb-c9c0b4701601#[使用者電子郵件地址]

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。

2024/04/17

未修補去年揭露CVE-2023-1389漏洞的TP-Link旗下Archer AX21無線路由器，持續被殭屍網路所利用

去年 TP-Link 旗下的無線路由器：Archer AX21(AX1800) 的 Web 管理介面被揭露存在一個未經驗證的命令注入漏洞 (CVE-2023-1389)。儘管該漏洞已被公告並提供修復，但仍有許多利用該漏洞的攻擊活動。最近觀察到的攻擊，利用各種殭屍網路，包括 Moobot、Miroi、AGOENT 和 Gafgyt。已知殭屍網路以物聯網漏洞為目標，因此使用者應安裝最新更新並遵循製造商的修復步驟。

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：

- CL.Downloader!gen277
- Linux.Mirai
- Trojan.Gen.NPE
- Trojan Horse
- WS.Malware.1

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

2024/04/17

CVE-2024-1852--WordPress WP-Membership會員外掛程式漏洞

CVE-2024-1852 是一個影響 WordPress WP-Members 會員外掛程式的高嚴重等級的跨網站腳本 (XSS) 漏洞。若被成功開採濫用此漏洞，可讓未經認證的攻擊者向受影響的網頁注入任意網頁指令碼。如果被管理員執行，開採濫用此漏洞還可能導致瀏覽該網站的訪客被重導向到惡意的網頁或進一步危害。該漏洞已在 3.4.9.3 版外掛程式中已得到解決。

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: WordPress WP-Members Membership Plugin CVE-2024-1852

2024/04/17

SoumniBot--安卓平台上的銀行金融惡意軟體，正在肆虐韓國

SoumniBot 是安卓平台上的銀行金融惡意軟體。據報導，該惡意軟體主要針對韓國手機／行動裝置使用者。SoumniBot 利用多種技術來逃避檢測，例如：無效的壓縮方法內容、檔案的容量異常以及檔名超級長的 XML 名稱空間。從功能上看，這款安卓惡意軟體可以收集受感染設備的資訊、連絡人資料、SMS／MMS訊息，並洩露儲存在設備上韓國銀行簽發的數位憑證。

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。

2024/04/17

Rincrypt勒索軟體

Rincrypt 是最近在威脅環境中又被發現的一個普通勒索軟體。它只會針對預定義清單的特定副檔名的檔案進行加密。被加密後會被冠上『.rincrypt』的副檔名。加密完成後，檔名為『READ THIS.txt』的勒索贖金支付說明文件檔會被放到受感染機器的桌面上。該檔案內容包含一個電子郵件地址，供受害者聯繫以獲取進一步指示操作。

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.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransomware!g10
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- WS.Malware.1

2024/04/17

傳播 XWorm遠端存取木馬(RAT)的網路釣魚行動，以繳稅相關議題為釣餌

據報導，有人透過網路釣魚行動，傳播 XWorm 遠端存取木馬 (RAT)。攻擊的最初始階段是以繳稅為幌子的 HTML 檔附件做為誘餌。若被開啓後，它會觸發一個 JavaScript 的檔案下載，然後執行一個 PowerShell 腳本。該腳本具有終止執行程序、管理誘餌 PDF 檔案、停用使用者帳戶控制 (UAC) 以及最終發送 XWorm 有效酬載等功能。

XWorm 可使攻擊者在未經授權的情況下存取設備，可竊取登錄憑證和密碼等敏感資訊。此外，它還具有剪貼簿監控、安裝勒索軟體和發起分散式拒絕服務 (DDoS) 攻擊的功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen572
- Scr.Malcode!gen
- WS.SecurityRisk.4

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。

2024/04/16

Risen勒索軟體

在真實網路情境上檢測到一個名為『Risen』的勒索軟體。根據其勒索贖金支付說明 ($Risen_Note.txt 和 $risen_guide.hta)，威脅者似乎採用雙重勒索策略，要脅如果不支付贖金，就會出售或洩露竊取的資訊。被加密後的檔案將按照以下格式冠上副檔名：[攻擊者的電子郵件地址，TELEGRAM：攻擊者的 ID].隨機 ID。受害者會被指定兩個電子郵件地址、一個 Telegram ID 和一個部落格網址 (架構在加密的 Tor 網站上) 作為聯繫方式。

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：

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

2024/04/16

防護亮點：最能兼顧安全與持續運轉～保護Microsoft SQL Server免受勒索軟體威脅的首選：Symantec Data Center Security

勒索軟體鎖定資料中心的攻擊正在竄升

勒索軟體威脅以多種不同的方式產生，並利用各種入口來入侵企業，但攻擊者越來越常用的一種方法是直接鎖定資料中心的伺服器和工作負載服務作為攻擊鏈的初始步驟。這些系統可能無法安裝建議的修補程式，通常還在繼續使用供應商早已不再提供更新的老舊的應用系統／程式，或者工作負載可能無法安排進行修補更新，以保持企業營運的持續性 (BCP)，避免由於任何停機時間而導致的風險。因此，資料中心環境遭受網路攻擊和勒索軟體活動的風險非常高。入侵單個資料中心可以存取多個相互連接的系統和應用程式，進而將攻擊的潛在影響最大化。

資料庫工作負載承載著企業的敏感性資料，為關鍵任務業務提供服務動能，所以成為勒索軟體攻擊者竊取資料並透過加密關鍵資料檔案勒以索贖金的重要目標。雖然有許多不同的資料庫應用程式，但 Microsoft SQL Server 是全球最受歡迎的資料庫之一，也是勒索軟體最虎視眈眈的目標，這主要是因為它部署在 Windows 平台上，攻擊者在 Windows 上有大量惡意軟體工具可用作有效酬載，也有一些可以利用就地取材攻擊 (living off the land)。

微軟的 SQL Server--主要的攻擊目標

最近報告凸顯一種模式，即勒索軟體攻擊者將 Microsoft SQL Server 作為其進入資料中心的開端。沒有妥善配置的 SQL 伺服器和薄弱的管理員密碼為暴力攻擊或 SQL 注入攻擊另闢蹊徑，讓未經授權的存取和資料外洩常常不費吹灰之力。遭入侵的系統可能會被用作存取點出售給其他方，或用於安裝額外的惡意有效酬載，最終實現資料滲出或金錢勒索。最近，美國網路安全暨基礎設施安全局 (CISA)，通令軟體發行商採取預防措施消除 SQL 注入漏洞，這突顯出企業需要特別注意 Microsoft SQL 伺服器的安全性。CISA 的通令是針對檔案傳輸應用程式 MOVEit 中的 SQL 注入漏洞發出的，該漏洞已被 CL0P 勒索軟體利用來做遠端執行程式碼。

針對 Microsoft SQL Server 的一些著名網路威脅活動包括

- Mimic勒索軟體 (Mimic ransomware)，透過對暴露的 Microsoft SQL 伺服器進行暴力攻擊獲得初始存取權限
- Mallox 勒索軟體，使用字典暴力攻擊進行初始存取嘗試，然後執行 cmd shell 進行進一步活動
- CLR SQLShell，類似於用於在 Microsoft SQL 伺服器上執行 shell 命令的 xp_cmdshell 預存程序
- CL0P 勒索軟體利用 MOVEit 檔案傳輸應用程式中的 SQL 注入零日時差漏洞 CVE-2023-34362，安裝名稱為 LEMURLOOT 的 web shell。
- Freeworld 勒索軟體是 Mimic 的新變種，也是透過暴力手段存取不安全的 Microsoft SQL 伺服器
- Bluesky 勒索軟體還透過暴力登入 sa 帳戶獲得初始存取權限，然後啟用 xp_cmdshell 預存程序來執行 shell 命令

Data Center Security--有效的解決方案

賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：提供一種全面的縱深防禦方法，可確保 Microsoft SQL 伺服器和底層作業系統的安全。我們的解決方案能夠有效提供零時差保護，抵禦日益猖獗的勒索軟體攻擊和其他針對資料中心環境的網路威脅。

為Microsoft SQL Server量身打造的DCS沙箱

專用於 Microsoft SQL Server 的賽門鐵克 sym_win_hardened_sbp 強制政策具有最小權限原則建構的內建 DCS 沙箱 (mssqlsrv_ps)，用於鎖定 Microsoft SQL 工作負載：

- 網路控制為用戶端應用程式與受信任的網路和設備之間定義其邊界，以限制其初始存取。此外，您也可以只讓可接受的通訊埠上進行網路連接。
- 啟用軟體執行控制後，可防止在未經授權的情況下任意執行命令直譯器，例如：cmd.exe、cscript.exe。這可以有效防止利用系統命令進行惡意活動的就地取材攻擊，並防止接觸 C&C 伺服器下載有效載荷和進一步的命令。
- 軟體安裝限制和作業系統限制可防止任何企圖常駐以便後續存取和對關鍵 Windows 作業系統資源篡改的行為。
- 程序存取控制防止使用 procdump 或 Mimikatz 工具轉存 LSASS。
- 受保護應用程式控制可確保在信任 MS SQL 程序執行的同時，它們不會被用來安裝批次檔、powershell 腳本、Cobaltstrike、Mimikatz 等工具和勒索軟體程式類型的惡意軟體有效酬載。

Symantec Windows Baseline Detection Policy

Symantec Windows Baseline Detection Policy 具有 Microsoft SQL Server 監控規則集，可提供 SQL 伺服器事件的可見性，並對可能的可疑活動發出警報：

- Microsoft SQL Server Login Activity Monitor 可審查 Microsoft SQL 伺服器 sa 帳戶的成功和失敗登入，有助於對暴力攻擊發出警報
- Microsoft SQL Server Service Activity Monitor 會列出 Microsoft SQL 服務的啟動和停止情況
- Microsoft SQL Server File and Registry Monitor 可即時監控任何篡改 SQL 伺服器檔案和註冊表資源的行為。

保護資料中心的環境，尤其是資料庫工作負載的安全非常重要。企業必須優先採取安全措施，包括及時安裝修補程式、強大的存取控制和持續監控，以降低勒索軟體滲透的風險，保護敏感性資料不被利用。這些開箱即用的賽門鐵克資料中心安全預設政策，可確保針對資料中心伺服器和工作負載入口點嘗試的上升趨勢提供強大的保護。

要了解有關賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。

2024/04/16

由TA558駭客組織所發起的SteganoAmor網路攻擊行動

一起被命名為 SteganoAmor 的新發動的網路攻擊行動被認為是 TA558 駭客組織所發動。攻擊者一直在利用隱寫技術，在影像檔中隱藏惡意程式碼。據瞭解，TA558 是一個以旅遊業和酒店業為目標的駭客組織，主要針對拉丁美洲的目標。在攻擊行動中，該組織繼續利用早在 2017 年就存在的 Microsoft Office Equation Editor 漏洞--CVE-2017-11882。觀察到的惡意酬載可能各不相同，包括 Remcos、Agent Tesla、Formbook、Guloader、Lokibot、Xworm 和其他幾個家族的惡意軟體。

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.Stealer!gen1
- SONAR.SuspLaunch!g13
- SONAR.SuspLaunch!g266
- SONAR.SuspStart!gen15
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Exp.CVE-2017-11882!g2
- Exp.CVE-2017-11882!g3
- Exp.CVE-2017-11882!g5
- ISB.Downloader!gen40
- Packed.NSISPacker!g14
- Scr.Malcode!gen
- Scr.Malcode!gen3
- Scr.Malcode!gen59
- Scr.Malcode!gdn33
- Scr.Malcode!gdn34
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Mdropper
- VBS.Downloader.Trojan
- Web.Reputation.1
- 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

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: Bad Reputation Application Connecting to Cloud Storage
- Web Attack: Malicious File Download 11
- 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。

2024/04/16
L00KUPRU勒索軟體

最近在真實網路情境發現源於 Xorist 勒索軟體的最新變種：L00KUPRU 勒索軟體。該勒索軟體會加密使用者檔案，並冠上 .L00KUPRU 的副檔名。攻擊者會以名為『HOW TO DECRYPT FILES.txt』的文字檔形式留存勒索贖金支付說明，並要求用戶使用比特幣支付贖金。此外，贖金支付說明的內容還顯示在桌面上的快顯視窗中，向受害者提供攻擊者的詳細聯繫方式以及用於付款的比特幣加密貨幣錢包的地址。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.CryptoTorLocker
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B

2024/04/16
SolarMarker惡意軟體攻擊行動採用PyInstaller進行混淆

據觀察，一個命名為 SolarMarker 的惡意軟體攻擊行動利用 PyInstaller 來混淆第一階段 PowerShell 腳本，而不是慣用的 Inno Setup 和 PS2EXE，凸顯攻擊者在此攻擊行動中逃避安全檢測機制方面隨機應變的功力。SolarMarker 通常透過尋引擎優化中毒／購買關鍵字排名廣告 (SEO-Poisoning) 的攻擊進行傳播。在這次觀察到的行動中，用戶受到誘惑，從一個冒充知名南加州醫科大學網站下載偽裝的 PDF 文件檔案。

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：

- 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。

2024/04/15

Hive0051c網路攻擊行動正在鎖定烏克蘭傳播GammaLoad惡意程式

據觀察，Hive0051c 網路攻擊行動正在鎖定烏克蘭以傳播 GammaLoad 惡意程式。攻擊的手法採用夾帶烏克蘭語的檔名附件釣魚電子郵件，目標是軍事和政府機構。GammaLoad 後門會帶來各種後續有效酬載的風險，而獨立的隱蔽式的備用 C&C 則為其提供已取得權限的保障。Hive0051c 利用多個管道的同步 DNS 流量來輪換基礎設施，並維持多個活躍的 C&C 備援機制。

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.MBT
- W97M.Downloader
- WS.Malware.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。

2024/04/15

魚目混珠：FatalRAT惡意木馬上架在假冒成加密貨幣交易APP的下載網站

發現一起全新的網路攻擊行動，攻擊者試圖透過偽裝成專為中國用戶設計的合法加密貨幣交易的 APP 下載網站傳播 FatalRAT 惡意軟體。一旦安裝了該惡意木馬的有效酬載，它就會竊取受害者的個人資訊並執行鍵盤側錄。

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-Net!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Coinbitminer!g1
- SONAR.SuspBeh!gen609

檔案型(基於回應式樣本的病毒定義檔)防護：

- Miner.Bitcoinminer
- Miner.Cpuminer
- SMG.Heur!gen
- Trojan.Coinbitminer
- Trojan.Gen.MBT
- 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

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。

2024/04/15

SpyNote遠端存取木馬，假冒成「測速照相APP」：法國司機遭殃了！台灣難道不會發生嗎？

測速照相機在法國相當普遍，作為道路安全措施的一部分，其數量近年來大幅增加。它們被部署在包括高速公路、城區和鄉村道路在內的不同地點，以監控和執行限速規定。這些測速照相機通常被安裝在超速或事故高發生地區，例如：學校附近、施工區和危險彎道。

此外，法國還採用由執法人員操作的移動式測速照相機或車輛上的自動系統。這些移動式測速照相機可以移動到不同的地點，針對不能容忍超速的特定區域或事件進行拍攝與舉發。

隨著這些嚇阻超速措施的加強，許多手機 APP、社群和網站如雨後春筍般出現，以告知司機測速照相出現的位置。眾所周知，網路犯罪分子一直在關注那些很容易以社交工程得逞的議題，進而鎖定大量受害者。

賽門鐵克最近發現，有人將 SpyNote(一種遠端存取木馬) 偽裝成「anti radar」的APP。該假冒 APP 可能聲稱能夠向司機發出關於測速相機和交通執法區域出現的警告。

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

2024/04/15

安卓平台上歷久彌新的惡意軟體：XploitSPY

一個被命名為「eXotic Visit 」的網路攻擊行動正在傳播安卓平台上客制化過的 XploitSPY惡意軟體的新變種。據報導，該行動早在 2021 年就開始，一直在傳播上架在特定的網站或 Google Play 商店上。最新變種新增及強化混淆、模擬器檢測等功能以及使用原生程式庫來隱藏攻擊者資訊。XploitSPY 具有從遭入侵裝置中擷取通話記錄、連絡簿和簡訊內容的功能。它還可以拍照、錄音或發送簡訊等功能。

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

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。

2024/04/12

具有合法簽章的螢幕鏡像軟體藏有惡意後門程式

最近一份報告發現，安卓平台上的螢幕鏡像軟體：LaiXi 存在一個帶有簽章的後門。根據該報告，攻擊者濫用微軟 Windows 硬體相容性計劃 (Microsoft Windows Hardware Compatibility Program) 來獲得微軟簽章。該惡意套裝軟體含一個嵌入式免費代理伺服器，目的可能是監視和操縱網路流量。

沒有跡象表明該軟體供應商遭受供應鏈攻擊，也無跡象顯示他們有意圖引入惡意程式碼。

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.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：

- PUA.Gen.2
- Trojan Horse
- Trojan.Certbypass
- 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!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。

2024/04/12

LightSpy監控工具被植入惡意程式碼

LightSpy是一款模組化監控工具，其後繼變種支援安卓和 iOS 平臺。遭惡意軟體植入後具有滲出使用者私人資訊、GPS 定位資料、簡訊、通訊軟體的對話與傳輸資料、電話通話記錄等功能。LightSpy 還能全面跟蹤受感染設備上的瀏覽器歷史記錄、遠端執行 shell 命令和錄製 IP 語音 (VOIP) 通話內容。

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

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.Malapp
- 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。

2024/04/12

TA547駭客組織所發起的散播Rhadamanthys惡意竊密程式的網路攻擊行動

在真實網路情境新發現一起散播 Rhadamanthys 惡意竊密程式的網路攻擊行動，該行動是由 TA547 駭客組織所發起。該行動針對德國多個行業。在攻擊中，攻擊者利用內含惡意 .lnk 捷徑檔的 .zip 壓縮檔，這些檔案一旦被執行就會觸發 PowerShell 腳本，導致被攻擊的端點感染 Rhadamanthys 惡意竊密程式。部署的惡意軟體有效酬載具有多種功能，包括收集和外洩使用者機密資料，例如：憑證、cookie 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.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspStart!gen14

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen9
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.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

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 796
- 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。