保安資訊--本周(台灣時間2024/01/12)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 1,900 台受保護端點上總共阻止了 5,430 萬次攻擊。這些攻擊中有 82.2% 在感染階段前就被有效阻止：**(2024/01/08)**

- 在**9萬5,300**台端點上，阻止了**1,650**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬9,300**台端點上，阻止了**1,260**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬9,300**台**Windows**伺服主機上，阻止了**1,080**萬次攻擊。
- 在**5萬6,700**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,400**台端點上，阻止了**79萬8,400**次嘗試掃描在**CMS**漏洞。
- 在**3萬8,600**台端點上，阻止了**120**萬次嘗試利用的應用程式漏洞。
- 在**19萬6,000**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**5,800**台端點上，阻止了**160**萬次加密貨幣挖礦攻擊。
- 在**10萬300**台端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**682**台端點上，阻止了**27萬4,100**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 11.76 萬個受保護端點上阻止了總計 490 萬次攻擊。**(2024/01/08)**

- 使用網頁信譽情資，在 **105.4K** 個端點上阻止 **420** 萬次攻擊。
- 攔截 **25.9K** 個端點上 **560.2K** 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 **9.7K** 個端點上攔截 **134.9K** 次瀏覽器通知詐騙攻擊。
- 在 **396** 個端點上攔截 **24.6K** 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 **713** 個端點上阻止 **1.4K** 次技術支援詐騙攻擊。
- 在 **162** 個端點上阻止 **536** 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。

2024/01/11

利用愛心做壞事～駭客組織散播間諜程式對聯合國難民署的捐贈者下毒手

2023 年末，賽門鐵克觀察到一個駭客組織鎖定葉門講阿拉伯語的手機用戶為目標，這些手機用戶樂於向聯合國難民署提供援助，難民署是一個向難民、尋求庇護者、無國籍人士和境內流離失所者提供保護和援助的聯合國機構。該工作經費來自政府、個人和企業的自願捐款，在葉門這個因持續衝突和流離失所而面臨艱困人道主義危機的國家發揮著至關重要的作用。

該惡意 APP 式偽裝成一個 APP 安裝程式（دليل_دقيم_لدعم_نم_المفوضية_السامية .apk），謊稱可以提供如何支援聯合國難民署的資訊。受騙安裝此 APP 的使用者實際上會在其手機上部署一個名為『SpyNote』的安卓間諜軟體。

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：

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

2024/01/11

NoaBot--源於Mirai的全新殭屍網路

2023 年是加密貨幣市場谷底翻身的一年，儘管尚未達到 2021 年的高點，但很明顯已從 2022 年初的低迷中反彈。據報導，加密貨幣總市值從 2022 年年中不足 1 兆億美元猛增至 2023 年 12 月的 1.5 兆美元。網路駭客順勢抓緊難得大幹一筆的機會，已將重點轉向面向網際網路的 Linux 系統和物聯網 (IoT) 設備。

據報導，一個源於 Mirai 全新殭屍網路扮演著加密貨幣挖礦攻擊行動的要角。該殭屍網路配備蠕蟲自轉式傳播器和 SSH 金鑰後門等功能，可以下載和執行其他二進位檔案或傳播到新的受害者。在攻擊鏈的特定階段也會部署 XMRig 挖礦程式的最新修訂版本。

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：

- Linux.Mirai
- OSX.Trojan.Gen
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.SecurityRisk.3

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。

2024/01/11

以Slack安裝程式為幌子，實則傳播擴散Atomic竊密惡意程式(AMOS)

Atomic 竊密惡意程式又名 AMOS，是一種 macOS 平臺上常見的竊密惡意程式。該惡意軟體透過 Telegram 出售，通常透過惡意廣告傳播擴散。AMOS 具有外滲多種資料的功能，包括保護 Mac 存放 app 及網站密碼地方的 keychain 密碼、使用者工作檔案、cookie、瀏覽器資料、信用卡詳情、加密貨幣錢包……等。最近，AMOS 被偽裝成 Slack 應用程式的安裝檔進行傳播。網路駭客透過谷歌廣告引誘受害者免費下載該軟體。與之前的版本相比，新版的 AMOS 強化一些額外的程式碼混淆。提供下載 AMOS 的惡意下載頁面，還宣傳 Slack 軟體的 Windows 版本，這反過來又提供 FakeBat 惡意程式家族，該惡意程式可與駭客所設置的 C&C 伺服器通訊，並下載其它的惡意程式。

保安網路知識補充：Slack 是一個生產力平台，透過無程式碼自動化和 AI 為每位員工提供支援，讓搜尋和知識共享更順暢，並使團隊保持聯絡並更加投入。Slack 是個受到全球公司信任和使用者喜愛的平台。

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
- 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。

2024/01/11

日本View Card信用卡用戶成為新一波網路釣魚的覬覦目標

在日本，View Card 是日本鐵路東日本集團發行的一種信用卡，用戶可以方便地使用 Suica(預付電子錢卡) 乘坐電車等。最近，賽門鐵克發現新一波欺騙 View Card 服務的釣魚郵件。電子郵件內容提及信用卡使用情況，並誘使使用者點擊釣魚網址以查看和確認當前卡的使用情況。

- 電子郵件主旨：[View's NETサービス]ビューカードご利用確認 (*重要：必ずお読みください)
- 翻譯後的電子郵件主旨：[View's NET Service] View 卡使用確認 (重要：請務必閱讀)

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)。

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。

2024/01/10

MS-SQL用戶請小心～Mimic勒索軟體正在發動針對MS-SQL的網路攻擊

在真實網路情境發現被命名為 RE#TURGENC 的全新網路攻擊行動，利用 Mimic 勒索軟體攻擊 MSSQL 伺服器。攻擊者利用暴力破解方法入侵目標伺服器，借助 xp_cmdshell 程序執行遠端命令 (xp_cmdshell 讓 Sql server 以相同的服務帳務執行 Windows command，是一個會影響安全性的功能，因此 SQL SERVER 預設是關閉此功能)。它使用多種工具，例如：PowerShell 腳本、Cobalt Strike 滲透測試工具、windows 密碼獲取神器：Mimikatz、可以執行遠端電腦上指令的 PsExec、進階埠掃描程式和一些 AnyDesk 二進位程式。 Mimic 勒索軟體有效籌載利用第三方協力廠商的檔名搜尋引擎工具軟體『Everything』的 API，透過查詢並標記列為加密的特定檔案格式，來加快加密重要的檔案。

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：

- ACM.Untrst-RunSys!g1
- SONAR.SuspBeh!gen616

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Ransom.Gen
- Ransom.Mimic
- Ransom.Zombie
- Scr.Malcode!gdn32
- 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。

2024/01/09

阿爾巴尼亞議會遭受No-Justice(*無正義)資料破壞軟體(Wiper)攻擊

伊朗駭客利用 No-Justice(*無正義) 資料破壞軟體 (Wiper) 攻擊阿爾巴尼亞議會。攻擊者利用 Putty Link、Revsocks 和 Windows 2000 資源工具包等常用工具進行偵察、橫向移動，並將目標鎖定為電信業者。No-Justice 資料破壞軟體 (Wiper) 可執行多種操作，包括載入函式庫、接收 API 功能的位址以及最終徹底刪除電腦磁碟內容。

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：

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：

- PUA.Gen.2
- PUA.Gen.4
- Trojan Horse
- WS.Malware.2
- WS.SecurityRisk.3

2024/01/09
MobiDash惡意程式持續造成行動裝置的資安威脅

安卓平台上的威脅不僅充斥著間諜軟體、銀行帳號接管軟體、簡訊詐騙等惡意軟體。行動裝置使用者還受到各種類型的垃圾廣告軟體困擾，這些軟體可能相當煩人，而且具有侵擾性。MobiDash 就是其中之一，而且已經存在一段時間。

MobiDash 是一種模組化的廣告軟體，可以整合成到其他 APP 中，而不是以獨立 APP 存在。據瞭解，它透過合法 APP(主要是遊戲) 進行傳播，這些 APP 被重新組合後加入這個模組，然後發佈到第三方 APP Store 和網站上。如果使用者在不知情的情況下下載，就會面臨大量的彈出廣告和惱人的網址重轉向。另一個不適的副作用是耗盡電池。

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

2024/01/09
防護亮點：Hunters International(*獵人國際)勒索軟體

在過去幾個月裡，我們持續觀察到一些新的勒索軟體，駭客集團以世界各國各種規模的企業為目標。其中包括 Hunters International、Meow、DragonForce、Werewolves、Malekteam……等駭客集團。賽門鐵克不間斷監控這些攻擊者，無論他們是透過資料滲漏或檔案加密進行單一勒索手法，還是同時採用資料滲漏和檔案加密的雙重勒索伎倆。

在本篇防護亮點中，我們將介紹 Hunters International 駭客集團，該勒索軟體駭客集團在 2023 年底宣稱有多名受害者上了新聞，進入 2024 年後又聲稱有更多受害者。該駭客集團使用的勒索軟體似乎與惡名昭章的 Hive 勒索軟體之程式碼有密切相關，2023 年初美國 FBI 已瓦解 Hive 勒索軟體犯罪網路。

截至目前，Hunters International 駭客集團的全部策略、技術和程序 (Tactics, Techniques, and Procedures，TTPs) 仍未完成分析。不過，已知他們會在受害者的基礎架構內橫向移動，一旦發現他們認為有價值的目標，就會洩漏出敏感性資料並加密檔案--這是大多數雙重勒索贖的經典作案手法。

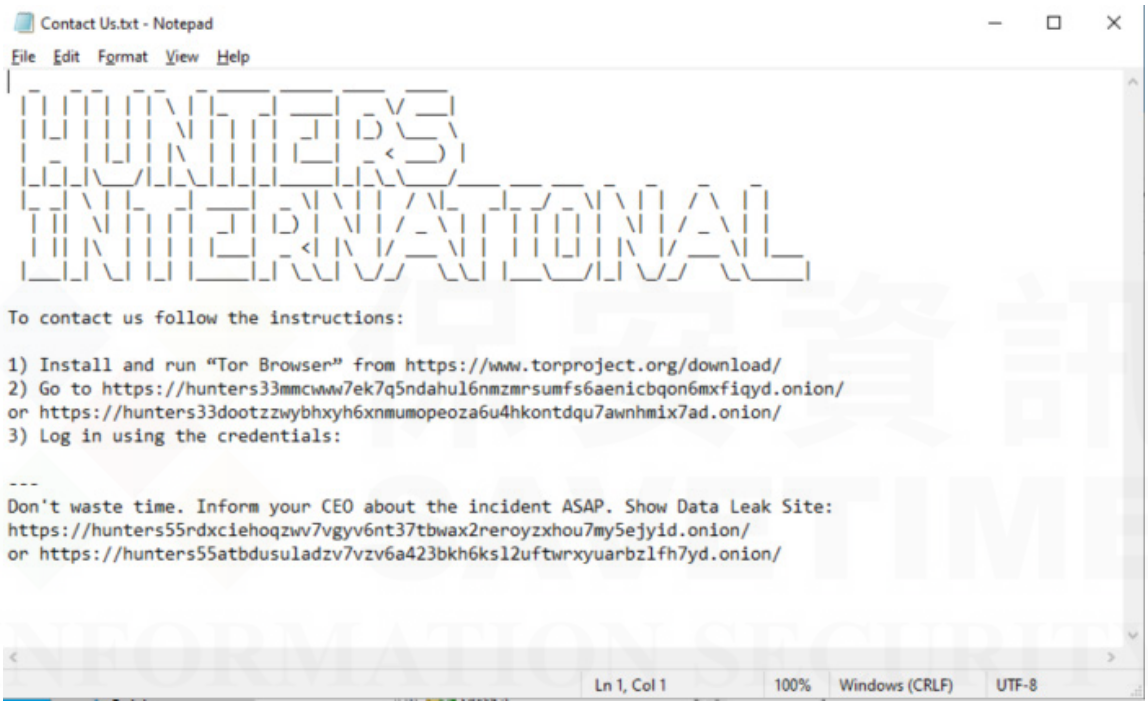
與之前的樣本類似，如果勒索軟體二進位檔案 (1 月份收集) 在遭入侵的機器上成功觸發，它將試圖停掉進程和服務。接下來，它會執行刪除備份和禁用回復機制的命令。然後，它會搜尋本機和對應磁碟機，以及透過 NetServerEnum 和 NetShareEnum API 在區域網路上發現的共用磁碟，並對發現的檔案進行加密。它會在每個加密檔案上冠上 .lock 附檔名，並在同一目錄下存放名為『Contact Us.txt』的勒索 (熟金支付) 說明。雖然目標是檔案加密，但它會跳過以下內容來加快重要檔案的加密速度：

- 包含以下字串名稱資夾內的檔案：$Recycle bin、$windows.~bt、$windows.~ws、all users

、appdata、boot、config.msi、default、google、intel、mozilla、msocache、perflogs、system volume information、tor browser、internet explorer、windows、windows.old、windows nt

- 檔名為：autorun.inf、bootfont.bin、boot.ini、bootsect.bak、desktop.ini、iconcache.db、ntldr、ntuser.dat、ntuser.dat.log、ntuser.ini.log、thumbs.db 的檔案
- 具有以下副檔名的檔案：386、adv、ani、bat、bin、cab、cmd、com、cpl、cur、deskthemepack、diagcab、diagcfg、diagpkg、dll、drv、exe、hlp、hta、icl、icns、ico、ics、idx、key、ldf、lnk、lock、mod、mpa、msc、msi、msp、msstyles、msu、nls、nomedia、ocx、pdb、prf、ps1、rom、rtp、scr、shs、spl、sys、theme、themepack、wpx

以下為受害者機器上留下的勒索(贖金支付)說明檔案內容截圖。



如上所述，賽門鐵克透過監控新的勒索／洩密網站以及來自外部和內部的其他資料，不斷追蹤新的勒索軟體攻擊者。雖然所使用的惡意軟體和工具並非現成或容易找到，但我們會繼續積極尋找樣本並識別所有 TTPs。這是一場持續的『貓捉老鼠』遊戲，保持資訊暢通和獲取入侵指標 (IOC) 是有效檢測和緩解威脅的關鍵要素。

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.Hunters!g1
- Trojan.Gen.MBT
- Trojan Horse

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g195

- SONAR.SuspLaunch!g253
- SONAR.RansomPlay!gen1
- SONAR.RansomGen!gen3
- SONAR.SuspLaunch!g193

基於機器學習的防禦技術：

- Heur.AdvML.B!100

基於安全強化政策(適用於使用DCS)：

Symantec DCS Hardening policy for Windows 可提供針對 Hunter's Hive 勒索軟體的 0-day 防護。預設沙箱可控制防止安裝 webhell 和惡意軟體工具，並防止特權應用程式執行任意系統命令。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序 (Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Ransomwares/HunterInternational/

欲深入瞭解有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。
欲深入瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。
欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲深入瞭解賽門鐵克 (DCS：Data Center Security～資料中心安全的更多訊息，請點擊此處。
欲深入瞭解賽門鐵克端點偵測與回應 (EDR) 的更多資訊，請點擊此處。

** 賽門鐵克端點偵測和回應（EDR）使用機器學習和行為分析來檢測和揭露可疑的網路活動。EDR 會對潛在的有害活動發出警告，對事件進行優先級別排序以便快速分類，並允許事件回應人員瀏覽裝置活動記錄，以便對潛在攻擊進行鑑識分析。

2024/01/09

CVE-2023-51467 Apache OFBiz繞過認證漏洞

CVE-2023-51467 是 Apache OFBiz (Open for Business 是一套功能齊全的企業自動化套件) 中的一個嚴重等級 (CVSS 評分為 9.8) 繞過認證漏洞。若被成功開採濫用漏洞會讓攻擊者繞過認證機制保護，並進行伺服器端請求偽造 (SSRF) 攻擊。Apache OFBiz 產品 18.12.11 或以上版本已修補此漏洞。

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：

- Web Attack: Apache OFBiz Authentication Bypass CVE-2023-51467

2024/01/09

Abyss(*深淵)勒索軟體

Abyss 是最近活躍在威脅領域的另一個勒索軟體。該惡意軟體會加密使用者檔案並冠上 .abyss 副檔名。加密完成後，會出現一個檔名為『WhatHappened.txt』的勒索 (贖金支付) 文字檔，說明如何下載 Tor 加密瀏覽器並聯繫攻擊者。此外，受感染機器的桌面背景也會被更改，以顯示勒索 (贖金支付) 說明。該惡意軟體具有刪除受感染機器上的磁碟陰影副本和系統備份的功能。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Untrst-RunSys!g1
- ACM.Wmic-DlShcp!g1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g193
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g340
- 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.2

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.C

2024/01/09

CVE-2023-22524-MacOS版Atlassian Companion中的遠端程式碼執行(RCE)漏洞

CVE-2023-22524 是最近揭露一個影響 Atlassian Companion for macOS 應用程式的遠端程式碼執行 (RCE) 漏洞。該漏洞被評級為嚴重等級漏洞，CVSS 評分為 9.6。若被成功開採濫用該漏洞會讓攻擊者利用 Websockets 雙向通訊協議繞過 Atlassian Companion 的黑名單和 MacOS Gatekeeper 的監控，在應用程式運行之前或隨後執行任意程式碼。該漏洞已在 2.0.0 或更新版本的產品中得到修補。

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：

- Web Attack: Atlassian Companion App for MacOS CVE-2023-22524

2024/01/08

觀察到AsyncRAT遠端存取木馬(RAT)所涉入真實網路情境的網路攻擊行動

據報導，在真實網路情境出現一個傳播 AsyncRAT 遠端存取木馬 (RAT) 惡意軟體涉入網路攻擊行動。幕後主使的駭客組織利用嵌入在釣魚網頁中 JavaScript 檔案傳播遠端存取木馬 (RAT)。

AsyncRAT 是一種開源遠端存取工具，自 2009 年起在 GitHub 上發佈，通常被用來作遠端存取木馬，也是最常用的遠端存取木馬之一。它顯著的功能包括鍵盤側錄、資料滲漏以及扮演發啟初始攻擊階段中傳遞最終有效籌載。

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：

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!gen569
- ISB.Heuristic!gen66
- Scr.Malcode!gdn14
- Scr.Malcode!gen105
- Trojan.Malscript
- Trojan Horse
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.A!300
- 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。

2024/01/08

macOS上的全新後門程式：SpectralBlur

BlueNoroff 駭客集團 (又名 TA444) 依然活躍，並持續推出新的 MacOS 惡意軟體系列。據報導，在最近一次的網路攻擊行動，該駭客集團佈署一個被稱為 SpectralBlur 的 MacOS 上全新後門程式。

SpectralBlur 惡意軟體後門整合檔案上傳和下載、檔案刪除、殼層執行和配置更新等典型功能。這些操作都是透過遠端命令與控制 (C&C) 伺服器的命令執行。SpectralBlur 的一個顯著功能

是使用偽終端遠端執行 shell 命令，這是以前從未見過的技術。SpectralBlur 與 KandyKorn (又名 SockRacket) 有相似之處，後者是一種精密複雜的植入程式，具有遠端存取木馬的功能，能夠控制被入侵的主機。

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

2024/01/08

Snake鍵盤側錄惡意程式涉入針對泰國企業的網路攻擊行動

雖然媒體並不常報導泰國的網路威脅情況，但它仍然相當活躍，世界各地的駭客組織與個體戶每天都在針對泰國的消費者和機構組織進行攻擊。在最近一個案例中，賽門鐵克發現一個『Snake Keylogger』惡意垃圾郵件散播行動，在該行動中，一名駭客試圖利用典型的『報價』社交工程伎倆，對在泰國設有辦事處或分公司的當地和國際公司進行攻擊。

惡意電子郵件 (主旨：**ขอใบเสนอราคา**) 包含一個 .ace 壓縮檔 (**รายละเอียด**.ace)，其中有一個 Snake Keylogger 二進位檔案 (**รายละเอียด**.exe)，偽裝成報價說明的假文件。在此攻擊行動中，主謀假冒兩家泰國公司，分別是上市的工程公司 (TTCL) 和食品包裝業公司 (Vexcel Pack)。

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)。

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

基於機器學習的防禦技術：

- Heur.AdvML.B!100

2024/01/08

網路釣魚行動中出現假冒亞馬遜Prime電子郵件通知

Amazon Prime 是亞馬遜 (Amazon) 推出的一項付費訂閱服務，為會員提供各種優惠。最近，賽門鐵克觀察到有人假冒亞馬遜 Prime 進行網路釣魚，誘使使用者打開虛假的通知郵件。郵件內容從『會員資格續訂』或『帳戶福利擱置』到帳戶安全警告不一而足。這些欺詐性電子郵件旨在誘騙使用者點擊釣魚網址。

- 電子郵件主旨： 您的 Prime 會員資格將重新續訂
- 電子郵件寄件者 "Prime" <偽造的電子郵寄地址>

點擊電子郵件內容中顯示的網路釣魚網址後，受害者就會被導引到憑據收集的釣魚網頁。

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)。

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。

2024/01/08

Linux平台出現Krasue遠端存取木馬(RAT)

第一次發現 Krasue 遠端存取木馬 (RAT) 惡意程式是在 2021 年。據報導，該惡意軟體主要針對泰國的組織，特別是電信部門。初始攻擊途徑可能包括暴力攻擊和開採濫用已知漏洞等。Krasue RAT 還嵌入支援各種 Linux 核心版本的匿跡惡意程式 rootkits。rootkits 偽裝成 VMware 驅動程式，用於隱藏惡意軟體活動軌跡、逃避檢測以及為攻擊者提供 root 存取權限。

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：

- Backdoor.Trojan
- Hacktool.Rootkit!gen8
- Trojan.Gen.NPE

2024/01/08

自帶漏洞驅動程式攻擊(BYOVD)～老牌LockBit勒索軟體在最新的網路攻擊行動中，打劫有機可趁的驅動程式瑕疵來停用安全軟體

LockBit 勒索軟體是一種廣受歡迎的勒索軟體即服務 (RaaS)，被賽門鐵克追蹤為 Syrphid 駭客集團所營運。雖然這個勒索軟體家族早在 2019 年就被首次發現，但每年都會出現新版變種。在賽門鐵克觀察到最新的網路攻擊行動中，LockBit 勒索軟體一直在濫用一種名為 TrueSightKiller 的工具。該工具開採濫用名為 truesight.sys 驅動程式的瑕疵，試圖停用安全軟體。該惡意軟體要求指定一個 PID(進程識別碼) 或進程名稱作為終止目標安全軟體的參數。

這類攻擊被統稱為『自帶漏洞驅動程式』(BYOVD：Bring Your Own Vulnerable Device)，源於授予具有合法數位簽章卻有瑕疵的驅動程式系統權限。BYOVD 攻擊一旦發生在受害者端點，主使者就可以在防毒軟體執行前的階段，就停用防毒或端點偵測與回應(EDR) 解決方案，所以在

進行檔案加密過程開始之前，安全軟體就沒有功效了。這也不是 LockBit 攻擊者第一次在勒索軟體攻擊行動中，打劫有機可趁的驅動程式瑕疵來停用安全軟體。早在 2022 年，他們就如出一轍地利用一個名為 Terminator 的類似工具。

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
- Ransom.Lockbit
- Trojan.Gen.MBT
- 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.C
- Heur.AdvML.B!200

基於端點偵測與回應(EDR)：

賽門鐵克的端點偵測與回應(EDR) 能夠監控和標記該幕後的攻擊者採用了全新的策略、技術和程序 (Tactics、Techniques、 Procedures，TTPs)。針對 TrueSightKiller TTP 的 EDR 增強規則包括：

- Subvert Trust Controls [T1553]
- Command and Scripting Interpreter: Windows Command Shell [T1059.003]
- Create or Modify System Process: Windows Service [T1543.003]
- Modify Registry [T1112]

賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多資訊，請參閱此鏈接：https://github.com/Symantec/threathunters/tree/main/Trojan/IcedID

2024/01/07

假冒DHL快遞服務的通知，網路釣客藉機竊取憑證

賽門鐵克發現，假冒 DHL 快遞服務的通知，網路釣客藉機竊取憑證有新的發展。在這一波攻擊行動中，網路釣魚電子郵件偽裝成貨運通知，在電子郵件主旨中顯示隨機提單號碼--這是貨運的常用參考號碼。電子郵件內容簡短，鼓勵收件人點擊釣魚網址。一旦點擊，受害者就會被引導至收集憑證的網頁。

- 電子郵件主旨：提單單碼 ***** - ([隨機的號碼])
- 電子郵件寄件者：DHL <假冒欺騙的電子郵寄地址>

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：

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)。

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。

2024/01/07

《寵物模擬器 99》玩家絞盡腦汁挖掘鑽石不慎感染勒索軟體

《寵物模擬器 99》是 BIG Games 在 Roblox 平臺上開發的《寵物模擬器》系列的第四部作品。遊戲靠著挖掘金幣和鑽石來獲得大寵，金幣用於孵化寵物。該遊戲於 2023 年 12 月 1 日推出，許多玩家絞盡腦汁使用自動打怪輔助程式來挖掘鑽石，卻在不知不覺中將自己置於風險之中。

在最近一次事件中，賽門鐵克發現一個透過瀏覽網頁不慎順道下載的社交工程伎倆，其中一個網路惡棍將 Chaos 勒索軟體偽裝成一個假冒的自動打怪輔助程式來挖掘鑽石。如果成功執行，該惡意工具將加密檔案，提示受害者透過電子郵件或 Discord 與攻擊者聯繫。

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
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- Heur.AdvML.A!300
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2024/01/05

Coper網路銀行惡意程式偽裝成谷歌的Chrome瀏覽器APP安裝程式

Coper 是 2021 年被發現安卓平台上的網路銀行惡意程式，最初目標是拉美國家的手機用戶，但多年來已蔓延到歐洲國家。截至目前，這種威脅仍相當活躍，最近賽門鐵克觀察到一個網路惡棍將 Coper 偽裝成谷歌的 Chrome 瀏覽器 APP 安裝程式 (GoogleChrome02.5.apk)，試圖以歐洲手機用戶為目標。它的功能包括收集敏感資訊、該惡意軟體可以生成螢幕疊加層並置頂以隱藏其惡意活動、欺騙使用者在不知情的情況下交出憑證等。

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

2024/01/05

善於偽裝的DiscordRAT(*不和諧鼠)遠端存取木馬(RAT)：從抖音機器人、電玩和深偽(Deepfake)軟體都是它的替身

DiscordRAT 是一種遠端存取木馬，在過去兩年中一直向大眾大肆宣傳，上架在一個知名的軟體發展者平臺上，允許他們保存、管理和協作程式碼。這個惡意程式並不特別流行，但總是時有耳聞，由其零星的活動中來判斷，它的感染途徑較多是透過瀏覽網頁不慎順道下載的社交工程伎倆。消費者大多是 DiscordRAT 攻擊的目標，但在某些情況下也會被用來攻擊企業用戶。

在最近活動中，這種惡意軟體被偽裝成許多不同的熱門工具和軟體，從抖音機器人、Fortnite 和 Valorant 等電玩安裝程式和汙衊人格的情色影片深偽 (Deepfake) 軟體都是它的替身。

不用多說，這款惡意軟體基本上可以讓攻擊者遠端控制受感染的電腦並竊取資訊。它可以顯示虛假資訊、執行命令、下載和上傳檔案，甚至操縱使用者介面。更令人擔憂是，它還能竊取密碼和開啟網路攝影機來擷取大頭照與錄影等資料，用 rootkit 隱藏自己的存在，甚至導致系統毀損。

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.B!100
- 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: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 656
- System Infected: Trojan.Backdoor Activity 721