保安資訊--本周(台灣時間2023/12/01)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 59 萬 9,300 台受保護端點上總共阻止了 6,840 萬次攻擊。這些攻擊中有 81% 在感染階段前就被有效阻止：**(2023/11/27)**

- 在**10萬1,800**台端點上，阻止了**2,450**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**17萬4,300**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**4萬1,100**台**Windows**伺服主機上，阻止了**1,180**萬次攻擊。
- 在**5萬8,200**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬1,400**台端點上，阻止了**84萬300**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,000**台端點上，阻止了**130**萬次嘗試利用的應用程式漏洞。
- 在**22萬3,700**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**1萬4,600**台端點上，阻止了**390**萬次加密貨幣挖礦攻擊。
- 在**11萬2,600**台端點上，阻止了**920**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**763**台端點上，阻止了**5萬5,500**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 1.443 萬個受保護端點上阻止了總計 610 萬次攻擊。**(2023/11/27)**

- 使用網頁信譽情資，在 **1.274** 萬個端點上阻止 **520** 萬次攻擊。
- 攔截 **32.3K** 個端點上 **648.4K** 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 **13.6K** 個端點上攔截 **165.3K** 次瀏覽器通知詐騙攻擊。
- 在 **632** 個端點上攔截 **59.9K** 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 **1.1K** 個端點上阻止 **2K** 次技術支援詐騙攻擊。
- 在 **222** 個端點上阻止 **512** 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。

2023/11/30

再怎麼維妙維肖終究還是贋品--精心策劃冒用法國財務總局(IGF)名義的網路詐騙正在肆虐法國

賽門鐵克發現一個垃圾郵件發送業者以法國境內的公司行號 (包括本地和境內跨國分公司)為目標，企圖冒用法國財務總局 (IGF) 的名義來詐騙 9,708.10 歐元。在法國，IGF 是『Inspection Générale des Finances』的縮寫，英文翻譯為『國財務總局』。它是一個政府機構，負責進行稅務稽核、審查並為法國政府提供諮詢服務。

惡意電子郵件（主址：『INSPECTION GENERALE DES FINANCES』）包含一個精心製作的 PDF 檔 (IMPOT(1)(1)-1.pdf)，冒充經濟部和財政部及 IGF 的公文。該電子郵件假借發現不實申報等違法行為，如果用戶不在 48 小時內支付罰款，他們可能面臨高達 500,000 歐元的巨額罰款和／或 5 年監禁。

該 PDF 檔還偽造現任行政和金融服務主管的簽名和蓋章，讓人很難識破--這是一個典型的偽造案例。這種恐嚇策略背後的組織或個人，希望受害者能與他們取得聯繫，如果聯繫上了，他們會提供相關繳交被設局受騙罰款的協助。

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)。

2023/11/30

澳洲高速公路收費系統LinkT的簡訊釣魚行動：偽造催繳單

由於繳費服務涉及金融交易、龐大的使用者群體和時間緊迫的先天條件，網路釣魚和欺詐行為者經常將繳費服務的使用者當作優先攻擊的目標。

繳費服務是金融交易的樞紐，對尋求金錢收益的網路犯罪分子很有吸引力。依賴繳費服務提供者提供交通服務廣大，使用者群為網路釣魚行動提供一個極具吸引力的目標，使攻擊者能夠接觸到不同的受眾並增加成功的機會。

催繳通知總是令人精神緊繃、緊迫感倍增，這也是網路釣魚攻擊能得逞的重要因素。受害者擔心逾期後果以及可能服務中斷，更有可能不加思索就匆忙回應網路釣魚企圖，從而讓攻擊者迅速獲取敏感資訊。

終究，繳費服務商必須透過各種管道與使用者聯繫，包括電子郵件、簡訊和電話。網路犯罪分子當然也會採用相同的聯繫方式來發動網路釣魚行動，提高社交工程伎倆的效率，進而增加成功的可能性。

澳洲高速公路電子收費 (ETC) 系統：LinkT，是賽門鐵克最近觀察到惡意簡訊攻擊行動的一個實例，威脅者透過虛假的催繳帳單通知將受害者引誘到釣魚網站。

觀察到的簡訊：

- Linkt:You have an unpaid vehicle invoice. 點擊 hxxps[:]//link[.]invoiceissue[.]cc 獲取更多資訊。
- Linkt:You have an unpaid vehicle bill. 點擊 hxxps[:]//link[.]ticketissue[.]cc 獲取更多資訊。

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。

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

人多扒手就多，網路上也一樣～耶誕假期，更多Afterpay用戶面臨網路釣魚與詐騙威脅

澳洲的先買後付 (Buy Now, Pay Later，BNPL) 新創公司：Afterpay，其提供的購物優惠以及齊備熱門商品，並可在六周內將其購物分成四次免息分期付款。這項服務在網路和實體商店都廣受歡迎，現在它是許多澳洲人的便捷支付選擇。

與這種服務相關的網路釣魚和網路詐騙幾乎不是什麼新鮮事，但在即將到來的耶誕假期，我們一定會觀察到更多的活動。其中一個例子，賽門鐵克發現一個惡意簡訊攻擊行動，該惡意行動試圖竊取 Afterpay 使用者的敏感資訊，並可能導致金融盜竊或詐騙。攻擊者假借帳戶出現問題等相關的社交工程伎倆和重定向到惡意網站的短網址引誘用戶。

觀察到的簡訊（原樣，包括『AfrerPay』錯別字）：

- AfrerPay：您的 Afterpay 帳戶有問題，請瀏覽以下網頁以利確認：hxxps://bit[.]ly/3Rj94Rz。

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。

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

Muck(*淤泥)竊密惡意程式

Muck 是主流的竊密惡意程式之一，其原始碼公開在眾所周知的軟體發展平臺上，很容易被公開取得。賽門鐵克目前觀察中的活動主要還只是在測試階段。現在判斷這種惡意軟體的流行程度還言之過早，但有一點可以肯定，它無疑會很快被一些駭客團體和個人以偷渡式下載的伎倆來傳播。

這種威脅主要針對 Discord 權杖、瀏覽器資料（cookie、密碼、歷程記錄、書簽、自動填表資訊、保存的信用卡）和加密貨幣錢包。它允許攻擊者使用 Webhooks 將竊取的資訊傳輸到 Discord。

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.Stealer!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan.Gen.MBT

2023/11/30

小心捷徑檔～遠端存取木馬SawRat，以捷徑檔開啟感染鏈

在真實網路情境觀察到一種以 Java 開發的全新遠端存取木馬 (RAT) 隱藏在 ZIP 壓縮檔中。由於該壓縮檔的檔名為『saw.chain』，所以該RAT 就被命名為 "Saw RAT"，該壓縮檔喬裝成具有 Adobe 圖示的捷徑檔(LNK)，誘使用戶打開一個看似 PDF 的檔案。當點擊該捷徑檔時，一個 JAR 檔會被打開並運行，它可以收集系統資訊、上傳檔案並在受感染的系統上執行其他命令。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- VBS.Dunihi!lnk
- WS.SecurityRisk.4

2023/11/30

Microsoft SharePoint Server的CVE-2023-29357漏洞正在被大肆開採濫用

CVE-2023-29357 是一個影響 Microsoft SharePoint Server 的嚴重等級（CVSS 評分 9.8）的提權 (EoP) 漏洞。如果成功開採濫用該漏洞，未經認證通過的遠端攻擊者可透過冒充認證用戶獲得存取權限。如果冒充的用戶帳戶是管理員帳戶，攻擊者就可取得管理員權限。

我們注意到有報告顯示，開採濫用該漏洞的事件在真實網路情境明顯增加。攻擊者正試圖從 SharePoint 伺服器中獲取使用者資訊，然後用於彙整管理員用戶清單來進一步偽造管理員身份。由此獲得的管理員權限還可用於進一步的漏洞利用來入侵網路。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，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：

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: Microsoft SharePoint Server Privilege Escalation CVE-2023-29357

2023/11/29

專門偽裝知名購物網站：Telekopye殭屍機器人已出現在真實網路情境

據報導，在真實網路情境已發現一個全新的殭屍機器人網路：Telekopye。Telekopye 是一個 Telegram 殭屍機器人被威脅行動者濫用在進行網路購物詐騙。該殭屍機器人的功能包括建立釣魚網站、發送釣魚郵件、簡訊和建立虛假截圖。威脅者利用這些機器人誘騙人們洩露個人資訊，例如：線上憑證和財務金融等相關資訊。在最近這次攻擊行動中，觀察到的主要目標是偽裝購物網站，例如：OLX、Yula、BlaBlaCar、eBay 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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- 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。

2023/11/29

Atlassian的DevOps協作平臺：Confluence存在CVE-2023-22518嚴重等級漏洞，已被大肆開採濫用

CVE-2023-22518 是 10 月被揭露的 Confluence 資料中心和伺服器中一個不當授權漏洞。如果成功開採利用漏洞，未經驗證的攻擊者可能會重設 Confluence 執行個體並建立新的管理員帳戶。使用此類帳戶，攻擊者可以對受感染的執行個體執行所有管理操作。就在本月，據報該漏洞在 Cerber 勒索軟體威脅組織的惡意行動中被開採濫用。

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: Confluence Broken Access Control Vulnerability CVE-2023-22515
- Web Attack: Confluence Improper Authorization Vulnerability CVE-2023-22518

基於安全強化政策(適用於使用DCS)：

賽門鐵克的 DCS(Data Center Security) 重要主機防護系統：其出廠就內建的強化政策就能完全提供零時差攻擊保護，針對該 Confluence 漏洞，能透過多種不同方式減少攻擊面和暴險。例如：鎖定 Confluence 在網路上的暴露，可防止網際網路上的攻擊。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2023/11/29

Xaro DJVU勒索軟體被夾雜在破解軟體安裝檔內的惡意程式載入器散播

在真實網路情境發現源於 Xaro 的 DJVU(又名 STOP) 勒索軟體的新變種。該惡意軟體由偽裝成免費軟體或破解軟體安裝檔的各種意程式載入器散播。該惡意軟體會對使用者檔案進行加密，並冠上 .xaro 的副檔名。加密完成後，檔名為「_readme.txt」文字檔案形式的勒索 (贖金支付) 說明將被存放到受感染的電腦上。威脅行動者索取 980 美元作為解密鎖定檔案的贖金。據觀察，最近散播 Xaro 攻擊行動還運行其他惡意籌載，例如：惡意竊密程式和網路銀行跟蹤程式 (Clipbankers)。

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.Untrst-Schtsk!g1

- SONAR.MalTraffic!gen1
- SONAR.ProcHijack!g21
- SONAR.SuspLaunch!g12

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Pots
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.2

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

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。

2023/11/29

持續看到Mallox勒索軟體在真實網路情境肆虐

Mallox 勒索軟體（也稱為 Fargo）是 TargetCompany 勒索軟體家族的要角，早在 2021 年就首次出現在威脅環境中。雖然它可能不像其他勒索軟體那麼普遍，但在 10 月於真實網路情境就已經看到新的 Mallox 樣本，11 月更證實該勒索軟體還繼續被用於惡意攻擊。Mallox 會加密使用者檔案並冠上 .mallox 副檔名。據了解，該勒索軟體幕後的威脅行動者不僅會加密檔案，還會從受感染端點中竊取機密資訊，以利後續採用雙重勒索伎倆。

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.SuspLaunch!g230
- SONAR.SuspLaunch!g309
- SONAR.TCP!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Ransom.Mallox
- 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.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：

- System Infected: Bad Reputation Process Request 4

2023/11/28

Jira軟體伺服器的CVE-2021-26086安全漏洞正被大肆開採濫用

Jira Atlassian 是全球企業最常用服務臺的工單 (ticketing) 工具之一。CVE-2021-26086 是 Jira 軟體伺服器中的一個目錄遍歷 (Directory traversal) 和檔案讀取漏洞。該漏洞允許遠端攻擊者讀取和外洩檔案等相關資訊。

賽門鐵克的網路防護技術入侵防禦系統 (IPS) 根據威脅狀況監控進行掃描，結果顯示開採濫用該漏洞的情況有所上升。攻擊者以包含敏感資訊 (例如：日誌資訊和配置設置) 檔案為外洩目標。這些被竊取的敏感資訊可被攻擊者用於進一步利用。儘管該漏洞已存在數年之久，但攻擊者仍希望利用企業延遲部署修補的空窗期大幹一票。

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 Jira Server File Disclosure CVE-2021-26086

2023/11/28

徵才與求職都是詐騙的好機會～兩起全新的進階持續威脅(ATP)網路攻擊行動都是以徵才與求職為幌子

研究人員回報兩起全新頑強駭客份子所發動的進階持續威脅 (ATP) 網路攻擊行動，分別稱為『Contagious Interview』和『Wagemole』。在『Contagious Interview』中，惡意駭客假扮成合法雇主徵求人才。在虛構的面試過程中，不知情的求職者會被誘騙安裝惡意竊密程式。

另一起則剛好相反，Wagemole 威脅行動者會冒充求職者，主要是美國組織的求職者，目的是從事網路間諜活動。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Malscript
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- 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。

2023/11/28

惡意軟體作者運用數學知識，試圖躲避沙箱攻擊偵測

安全研究人員最近發現，惡意軟體作者已開始改用三角函數來判斷當惡意軟體在內部運行時的嘗試與確認。利用一些繁複的三角函數，惡意軟體能夠追蹤滑鼠加速度，進而確定它是否在沙箱中運行，並改變其行為。

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

基於機器學習的防禦技術：

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

2023/11/28

漏洞永遠對威脅倘開大門，再久遠的漏洞也一樣～從XLA到RFT再到VBS：猶如瘟疫肆虐的拉丁美洲Agent Tesla垃圾郵件攻擊行動

賽門鐵克最近檢測到一個 Agent Tesla 垃圾郵件攻擊行動，主要針對幾個拉美國家，包括墨西哥、厄瓜多爾、多明尼加、哥倫比亞、巴西和秘魯。攻擊者開採濫用眾所周知且已釋出修補程式的久遠漏洞作為其發送機制。這些電子郵件帶有一個 XLA 檔附件（名為 boleto bancário.xla

或 cotización.xla）。執行後，該附件會利用 CVE-2017-0199 漏洞去下載惡意 RFT 文件檔。隨後，RFT 文件檔又開採利用 CVE-2017-11882 漏洞下載 VBS 檔（mondaybrazillll.vbs），最終導致部署 Agent Tesla 惡意軟體。

觀察到的電子郵件主旨：

- 付款
- 付款相關資訊
- solicitud de cotización...

CVE-2017-0199 是 Microsoft Word 和 Office Online 中存在的漏洞。它允許攻擊者透過包含嵌入式 OLE2link 物件的偽造文件檔執行任意程式碼，從而導致潛在的遠端程式碼執行。

CVE-2017-11882 是 Microsoft Office 2000／2003 的預設工具：可於文件中插入及編輯方程式的 Equation Editor 的記憶體毀損漏洞。開採濫用該漏洞，攻擊者可以透過惡意製作的檔案執行任意程式碼，為遠端代碼執行提供途徑。

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：

- Exp.CVE-2017-11882!g2
- Downloader
- Scr.Malcode!gen59

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

2023/11/28

BlackNet(*黑網)遠端存取木馬(RAT)在網路攻擊行動中展現十八般武藝

在全球範圍內，惡意軟體行動的主謀往往透過在攻擊鏈或惡意軟體本身中加入『復活節彩蛋』方式，影射或暗喻自己的觀點--無論是政治觀點、地緣政治觀點、宗教觀點還是激進主義觀點。在最近一個案例中，賽門鐵克在審查與以色列--哈馬斯緊張局勢有關的網路犯罪活動時，發現一個搭配 BlackNet 命令與控制伺服器 (C&C) 的網域，作者給它起一個與衝突密切相關的名字。

在過去幾年中，BlackNet 經常被多個駭客組織成員所使用。這種遠端存取木馬 (RAT) 具有在遭入侵系統上執行各種操作的能力，包括但不限於上傳檔案、執行腳本和 shell 命令、開啟網

頁 (可視和隱藏網頁)、截圖、從 Chrome 和 Firefox 等瀏覽器中竊取保存的密碼以及鍵盤記錄。這種惡意軟體主要透過惡意電子郵件傳播，但也可能透過偷渡式下載傳播。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Untrst-RLsass!g1
- ACM.Untrst-RunSys!g1

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

2023/11/28

防護亮點：入侵預防的稽核特徵(IPS Audit Signatures)--防範Discord和Telegram遭濫用的另一層數位監控系統

Discord 和 Telegram 是近年來大受歡迎的通訊和檔案分享應用程式。Discord 主要面向遊戲社群，提供各種迎合這一人群的功能，包括語音和文字聊天頻道、檔案分享和可定制性。Telegram 則是一款泛用性更強的通訊應用程式，它為訊息提供端到端加密，讓用戶可以安全地進行通訊。

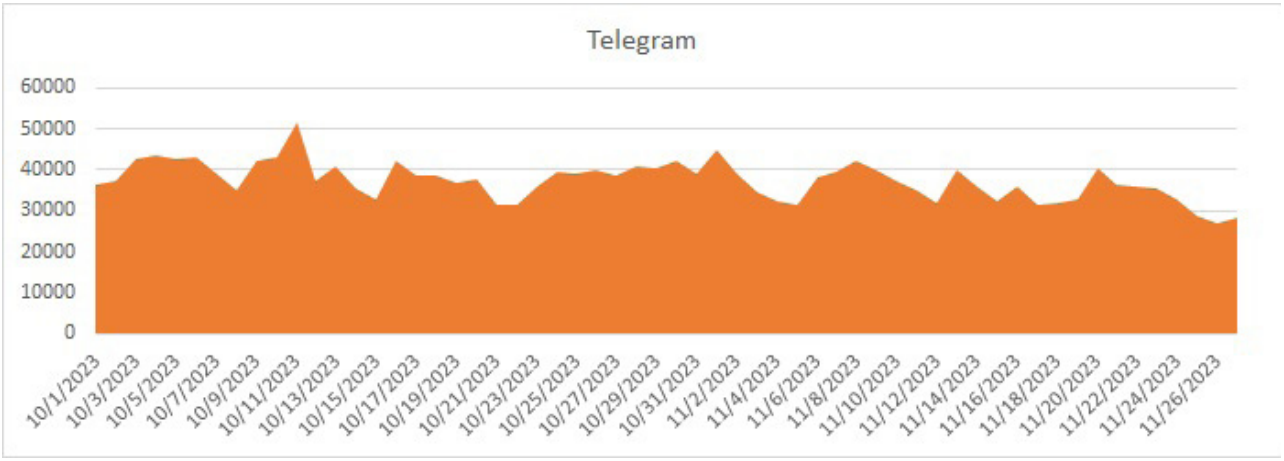
Discord 和 Telegram 的廣受歡迎，也自然成為網路犯罪分子覬覦的目標。造成這種趨勢的因素有幾個：

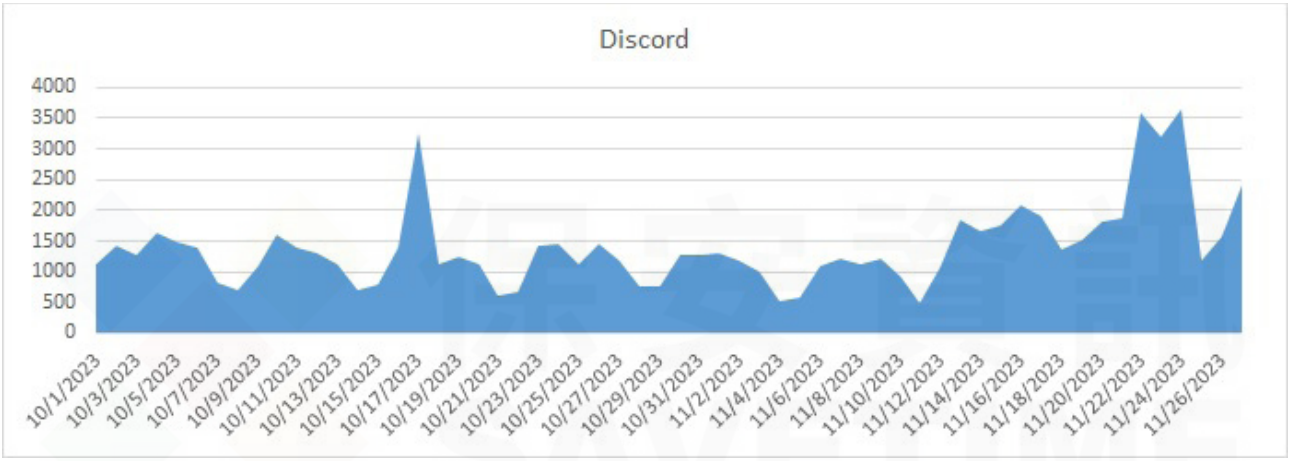
- **龐大的用戶群**：Discord 和 Telegram 都擁有數以百萬計的活躍用戶，這使它們成為網路犯罪分子試圖接觸廣大受眾的誘人目標。
- **檔案分享功能**：這兩個平臺都允許用戶輕鬆分享檔案，包括可執行檔，這些檔可用於傳播惡意軟體。
- **易於使用**：Discord 和 Telegram 都比較容易使用，這使得具有不同專業技術水準的用戶（包括那些懷有惡意的用戶）都能使用它們。
- **審核不易**：雖然這兩個平臺都實施一些審核措施，但由於使用者生成內容數量龐大，因此很難有效識別和刪除惡意內容。

由於這些因素，Discord 和 Telegram 已日益成為惡意檔案上架保管和竊取資訊外流的熱門途徑。網路犯罪分子濫用這些平臺分享惡意軟體、傳播被盜資料並從事其他非法活動。我們的讀者可在此處查看以前發佈的與可能利用 Discord 和／或 Telegram 威脅有關的防護公告。。

因應日益增多的惡意活動，除了更強大的防毒保護技術 (基於行為、啟發式和機器學習) 外，賽門鐵克還發佈幾款入侵預防 (IPS) 稽核特徵，以提供多一層的安全保護，讓客戶在監控未經稽核和可能被惡意行動者濫用的 Discord 和 Telegram 網路流量面向取得優勢。

賽門鐵克入侵預防的稽核特徵在過去兩個月內回報以下可疑活動：





SEP 的稽核特徵，讓您可以監控某些類型的流量，例如：Yahoo IM 登入。這些特徵預設為「不記錄」。您可以建立例外以記錄此流量，然後檢查日誌並決定如何處理流量。例如：您可能想要為該流量類型建立防火牆規則。

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：

- Audit: PowerShell Process Accessing discordapp
- Audit: System Process Accessing discordapp
- Audit: Untrusted Telegram API Connection

若要進一步瞭解什麼是入侵預防 (IPS) 及其用途以及如何使用 URL 信譽攔截勒索程式？請參閱：管理入侵預防。

2023/11/28

GhostLocker勒索軟體

GhostLocker 是一種以『按需付費的勒索軟體攻擊即服務』(RaaS) 營運模式散播的勒索軟體，本月已在真實網路情境被發現。GhostLocker 具有延遲加密、提權和終止遭入侵電腦上的程序和服務等功能。加密完成後，會被冠上 .ghost 的副檔名。多數的 GhostLocker 最新變種都是採用 Nuitka 編譯，這是一種從 Python 程式碼轉移到 C 二進位檔案的原始碼對接編譯器。

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
- SONAR.Dropper

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。

2023/11/28

RisePro惡意竊密程式新變種新增遠端存取木馬(RAT)功能

據瞭解，RisePro 是一種惡意竊密程式，透過 PrivateLoader 惡意軟體載入器以熱門軟體的破解版為幌子進行傳播。該竊密程式覬覦的目標是受感染端點上的 cookie、保存的憑證、銀行資訊和加密錢包。RisePro 的最新變種也展示一些類似 RAT 的附加功能，並使攻擊者能夠遠端控制遭入侵的電腦。為此，該惡意軟體利用 HVNC (隱藏虛擬網路連線) 與威脅行動者進行通訊。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-Schtsk!g1
- SONAR.Heuristic.159
- SONAR.SuspStart!gen15

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.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: Trojan.Backdoor Activity 634
- System Infected: Trojan.Backdoor Activity 656

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。

2023/11/27

法國和瑞士出現RedProtection勒索軟體

RedProtection 是 chaos 勒索軟體的一個變種，最近在法國和瑞士被發現流傳。一旦加密成功，它就會部署一張用英語和法語書寫的贖金條。受害者被要求在 24 小時內向指定的加密貨幣錢包轉帳 0.0061 BTC，然後通過 Telegram 聯繫攻擊者。說明中還提到願意就贖金金額進行談判。該威脅行為體專門針對企業使用者和消費者的個人電腦。

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-RLsass!g1
- ACM.Untrst-RunSys!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Sorry

2023/11/27

推波助瀾～惡意軟體載入器DBatLoader助長Formbook多功能惡意程式在西歐和東歐氾濫成災

賽門鐵克觀察到一個濫用惡意軟體載入器 DBatLoader (也稱為 ModiLoader) 來針對歐洲和東歐機構／組織發動的網路攻擊行動，其攻擊者冒充包括克羅埃西亞一家銷售和租賃帳篷、帳篷和舉辦活動所需相關設備的企業、保加利亞一家非營利性研究型製藥商協會以及土耳其一家生產和銷售混凝土產品的公司……等。

惡意電子郵件包含一個內含 DBatLoader 二進位檔案（例如：Kopija bankovne uplate.exe）的壓縮檔。如果用戶被成功誘騙執行該壓縮檔，就會啟動 Formbook多功能惡意程式，攻擊者採用『付款』主題的社交工程伎倆雖是老套，但依然有效。

郵件主旨：

- otvrda uplate
- Վճարում
- ödeme onaylama

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：

- ACM.Ps-RgPst!g1
- SONAR.Stealer!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

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.Formbook Activity 5
- System Infected: Trojan.Formbook Activity 2
- Web Attack: Webpulse Bad Reputation D

2023/11/27

明察秋毫～賽門鐵克近期又發現Raptor(*猛禽)--安卓平台上的遠端存取木馬(RAT)及其呼應C&C 伺服器

賽門鐵克發現一個駭客集團或個體戶所營運的一個名為『Raptor』安卓平台上的遠端存取木馬 (RAT) 和一個命令與控制 (C&C) 伺服器。這種威脅並不新鮮，已經流傳幾年。有興趣的人可以透過論壇、網站和軟體發展平臺上的留底取得其原始碼。

如果在受害者不知情的情況下成功安裝這種惡意程式，它就會向其 C&C 伺服器回報並等待威脅者的命令。該惡意軟體可使作者透過 Webhooks 向 Discord 檢索和外洩竊取的資訊。其功能列表包括：

- 收集敏感資訊（簡訊內容、設備和位置資料、通話記錄、連絡人、應用程式清單、檔案、瀏覽器歷史記錄等）
- 發送高資費詐騙簡訊
- 刪除 SD 記憶卡上內容
- 鎖定螢幕和變更桌布
- 使用 AES 金鑰『0123456789012345』加密所有圖片和媒體檔案
- 震動設備、刪除通話記錄和啟動語音資訊

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。

- Android.mobilespy

2023/11/27

北韓網軍Lazarus發動～訊連科技(CyberLink)供應鏈攻擊

從合法軟體源頭下手是非常精密且隱匿的惡意軟體傳播方式。因為，毫無戒心的受害者就會從合法來源更新他們合法軟體。在受害者不知情的情況下，軟體表面上會正常運行，但卻會讓惡意行動者駭入系統，或執行任何其他邪惡行為。這就是所謂的供應鏈攻擊伎倆。最近研究發現，被名為 Diamond Sleet（又名 Lazarus、Appleworm、ZINC）威脅行動者動過手腳的 CyberLink 安裝程式版本就是這種情況。

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
- Web.Reputation.1
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2023/11/27

BlackoutWare勒索軟體

BlackoutWare 是最近在真實網路情境有人回報的另一種普通勒索軟體。該惡意軟體會加密使用者檔案，並冠上 .blo 副檔名。勒索 (贖金支付) 說明以檔名為『WARNING.txt』的文字檔形式提供，攻擊者要求受害人用萊特幣或比特幣支付等值於 5000 歐元的贖金，以獲得資料解密。該惡意軟體還具有磁卷陰影複製 (volume shadow copies) 的破壞力。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.RansomNokibi!g1
- SONAR.SuspLaunch!g18

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen
- 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

2023/11/27

偽裝欺敵～Irata 惡意程式偽裝成阿拉伯語股票APP

Irata (又名伊朗遠端存取木馬) 是一款具有間諜軟體功能的安卓平台上的惡意銀行 APP，至少從 2022 年開始就一直活躍在行動威脅領域。賽門鐵克最近檢測到其活動有所增加。在一次攻擊行動，幕後的駭客集團或個體戶將其惡意二進位檔案 (saham.apk) 偽裝成阿拉伯語使用者的股票手機應用程式 (APP)。

觀察到的 APP 保存上架在惡意域名上，這很可能表明它們是透過惡意簡訊而非官方或第三方協力廠商應用程式商店傳播。據瞭解，這種作案手法是 Irata 威脅行動者慣用的伎倆。

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。

2023/11/26

採Rust改寫的的全新版本SysJoker惡意軟體

據報導，與哈馬斯有聯繫的威脅分子利用一種名為『SysJoker』基於 Rust 的新型多平臺惡意軟體發起一場進階持續威脅 (APT) 網路攻擊行動。該變種雖然改寫源於早先基於 C++ 的程式碼的版本而來，但仍保留原有功能，例如：收集受害者的電腦資訊（包括作業系統版本和 MAC 位址等），並透過 OneDrive 回傳至攻擊者所操控的 C&C 伺服器。

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：

- 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

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 (33246)

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。

2023/11/26

敢用刀子命名的惡意程式應該有兩把刷子～KratosKnife(*克瑞托斯刀)殭屍電腦惡意軟體

KratosKnife 是一種已經存在數年的殭屍電腦惡意軟體，已在多個網站、論壇以及公開的線上版本控管服務上分享。從流行程度上看，該惡意軟體與最活躍的具有相同功能（殭屍電腦惡意軟體和竊密惡意程式）的威脅相比，可謂小巫見大巫，但賽門鐵克仍能觀察到惡意或與測試相關的零星活動。惡意攻擊幕後的駭客集團或個人通常透過瀏覽網頁時常見的順道下載伎倆為初始感染媒介。一旦成功入侵，就能部署額外的有效籌載、執行命令並收集各種敏感資訊（cookie、加密錢包等）。

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：

基於行為偵測技術(SONAR)的防護：

- ACM.Untrst-RunSys!g1

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.A!300
- Heur.AdvML.C

2023/11/24

又是勒索軟體～Messec勒索軟體

Messec 是最近在真實網路情境觀察到另一個源於 Chaos 勒索軟體的新變種。該惡意軟體會加密使用者檔案，並冠上 .messec 副檔名。並留下『READ_ME.txt』文字檔的的勒索 (贖金支付)說明，攻擊者要求用比特幣支付 100 美元贖金才能解密資料。一旦入侵電腦上的檔案被加密，惡意軟體還會更改電腦的桌面背景圖案。

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：

- SONAR.SuspDrop!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!200

2023/11/24

ParaSiteSnatcher利用Chrome瀏覽器擴充功能入侵銀行資料

ParaSiteSnatcher 是一個新發現的框架，它利用 Google Chrome 瀏覽器擴充從遭入侵的端點進行資料外滲。在最近針對拉丁美洲用戶的攻擊行動中，威脅分子一直在使用 ParaSiteSnatcher，並竊取與巴西銀行和聯邦經濟銀行（Caixa Econômica Federal，Caixa）有關的使用者銀行資訊。該惡意軟體具有操縱 PIX（巴西支付系統）交易和 Boleto Bancario（另一種支付系統）的功能。ParaSiteSnatcher 透過保存在公共雲存儲庫中的 VBS 下載程式進行傳播。

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：

- ISB.Houdini!gen7
- Scr.Malcode!gen114
- Trojan Horse
- Trojan.Gen.NPE.C
- Trojan.Malscript

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。

2023/11/24

編號CVE-2023-46604的Apache ActiveMQ遠端程式碼執行(RCE)漏洞，已被Kinsing 挖礦劫持惡意軟體開採利用

CVE-2023-4660 是最近揭露的 Apache ActiveMQ 上嚴重等級 (CVSS 評分：10) 遠端程式碼執行 (RCE) 漏洞。根據最近報告，與 Kinsing 挖礦劫持惡意軟體有關的威脅行動者正在大肆開採利用這一漏洞滲透和入侵 Linux 系統。Kinsing 惡意軟體透過開採利用網路應用程式中的漏洞或容器環境中錯誤配置進入系統。一旦系統被感染，惡意軟體就會迅速擴散到整個網路，對整體安全構成重大威脅。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Malscript!g1
- 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: Apache ActiveMQ RCE CVE-2023-46604

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。