保安資訊--本周(台灣時間2024/08/09)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 50 萬 3,100 台受保護端點上總共阻止了 5,031 萬次攻擊。這些攻擊中有 81.8% 在感染階段前就被有效阻止：**(2024/08/05)**

- 在**9萬2,200**台端點上，阻止了**1,190**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬5,100**台端點上，阻止了**940**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬3,400**台**Windows**伺服主機上，阻止了**84**萬次攻擊。
- 在**5萬6,700**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬900**台端點上，阻止了**71萬6,700**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,600**台端點上，阻止了**330**萬次嘗試利用的應用程式漏洞。
- 在**15萬1,800**台端點上，阻止了**350**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**5,300**台端點上，阻止了**110**萬次加密貨幣挖礦攻擊。
- 在**10萬2,200**台端點上，阻止了**770**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**703**台端點上，阻止了**8萬3,900**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 萬 1,700 個受保護端點上阻止了總計 340 萬次攻擊。**(2024/08/05)**

- 使用網頁信譽情資，在 **102.9K** 個端點上阻止 **290** 萬次攻擊。
- 攔截 **19.8K** 個端點上 **414.2K** 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 **6.2K** 個端點上攔截 **82.4K** 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 **227** 個端點上攔截 **6.3K** 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。

2024/08/08

勒索軟體威脅份子鎖定英語系和西班牙語系的Linux電腦發動攻擊

賽門鐵克最近觀察到一個 Linux 平台上的勒索軟體的二進位檔案，似乎是針對英語系和西班牙語系用戶的雙重勒索攻擊。目前，他們的作案手法仍不清楚，但該勒索軟體呈現以下行為。

- 勒索贖金支付說明文字檔存放在 /root/README.txt 和 /user/[username]/README.txt 中，指示受害者後續的步驟。
- 包括 PostgreSQL、MongoDB、MySQL、Apache2、Nginx 和 PHP-FPM 在內的關鍵程序和服務會被強制停用，以防止攻擊受到任何干擾。
- /etc/motd 檔案會被覆寫警告訊息，"Your files have been stolen and encrypted. Read README.txt for more information.(*明「您的檔案已被竊取並加密。閱讀 README.txt 以獲得更多資訊」)"。
- 勒索軟體加密磁碟上的檔案

勒索贖金支付說明文字檔本身包含英文和西班牙文，建議受害者使用「Session」與他們聯繫--這是一款注重隱私的訊息應用程式，目的在提供安全、匿名的通訊，同時不影響可用性。以下是勒索贖金支付說明文字檔的摘錄：

中文意思大致如下(分別有英文版本及西班牙文版本並列)：
您的檔案已加密並下載至我們的伺服器。
如果沒有我們的解密軟體，您的檔案將無法解密。
我們擁有 TB 級的貴公司資料，包括員工電子郵件、員工密碼和客戶資料庫。
若要防止這些資料外洩並取得解密軟體，請使用下列其中一種方法與我們聯絡：

Session (hxxps[:]//getsession[.]org)
ID: [已刪除]
hxxps[:]//getsession[.]org/blog/session-for-beginners"

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.Gen

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security其出廠就內建的系統鎖定政策，可以保護底層的作業系統免受此漏洞的侵擾。DCS 的網路規則政策可設定為，將 ActiveMQ 應用程式限制為受信任的用戶端。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2024/08/08

以加密貨幣為訴求的誘騙網站被用發動網路釣魚攻擊

威脅份子正在製造數千個加密貨幣主題的誘騙網站，用於針對 MetaMask、WalletConnect、Coinbase、Trezor、Ledger、Bitget、Exodus、Phantom 等加密貨幣錢包品牌的使用者進行網路釣魚攻擊。這些威脅份子濫用 Gitbook 和 Webflow 等免費託管服務以疑似的域名來建立誘惑網站，例如以下網站：

- metamask---data-wallet.webflow[.]io
- connected----wallet.gitbook[.]io
- content--walet-coinbs.gitbook[.]io
- wallet-trezorhardware - help.gitbook[.]io
- content--ledger-wallet.webflow[.]io

這些網站以加密錢包的相關資訊和下載連結引誘潛在受害者，但實際上這些連結會指向類似以下的惡意網頁：

- antressmirestos[.]com/9616d14f-fbe8-441d-b9d6-0c96aad8512
- egaiterimturches[.]com/ae9f2bf6-7377-4cc9-a730-11613f03920
- clistationsomminder[.]com/5c5756fa-cf78-47a3-9515-65e216d503c8

這些網頁可作為惡意流量分配系統 (TDS)，將使用者重導向至網路釣魚內容，或在系統認為使用者是安全研究人員時，將使用者重導向至良性內容。

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：

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。

2024/08/08

全起新型惡意垃圾郵件行動，散播多種木馬程式

許多惡意垃圾郵件攻擊行動透過嘗試開採濫用 Microsoft Office 的老舊漏洞來散播各種特洛伊木馬程式。CVE-2017-0199 漏洞仍然是讓 XLS 檔案有機會執行遠端程式碼的破口。這些惡意行動會傳送惡意的 XLS 檔案，並附有連結，進而執行遠端 HTA 或 RTF 檔案以下載最終的有效酬載。我們觀察到的有效酬載是 GuLoader 惡意程式載入器、Remcos 遠端存取木馬和 Sankeloader 惡意竊密程式。

主旨範例(中文意思)：

- 新的 RFQ PO1752
- 付款通知 - 通知編號

檔案附件名稱範例：

- HSBC Advice_ACH_Credit_08072024.xls
- Pepsico Company Profile.xls
- Quotation.xls
- RFQ Data Sheet Technical Specifications Conditioning System Package.xls

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.Stealer!gen1
- SONAR.TCP!gen1

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：

- Scr.Malcode!gdn33
- Scr.Malcode!gdn34
- Scr.Malcode!gen59
- Trojan.Gen.MBT
- Trojan.Guloader

基於機器學習的防禦技術：

- 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。

2024/08/08

還是用騙得比較快～以AI驅動的Sora前瞻性工具為幌子的惡意軟體散播行動

威脅份子已建立各種冒充官方 Sora 平台的釣魚網站，誘使受害者下載偽裝成合法 Sora 軟體的檔案，以散佈有害的有效酬載，包括資料竊取器和惡意挖礦程式。當使用者嘗試安裝被誤認為是正版的應用程式時，這些檔案會觸發惡意程序，入侵受害者的系統。與資訊竊取相關的多項任務都會被觸發，其中敏感資訊會被滲出，例如：Cookie、登入憑證和各種瀏覽器的自動填入資料。

網路知識：Sora 是 OpenAI 在繼 ChatGTP/GPT-4 後最新推出的一項前瞻性工具，能夠運用先進的人工智慧技術將文字轉換為影片。

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-CPE!g2
- ACM.Ps-FlPst!g1
- ACM.Ps-Http!g2
- ACM.Ps-RgPst!g1
- ACM.Ps-Wscr!g1
- ACM.Any-Pyarmor!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Miner!gen2

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.XMRig!gen1
- Infostealer
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- WS.Malware.1

基於機器學習的防禦技術：

- 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。

2024/08/08

假冒英國安全衛生執行署(Health and Safety Executive，HSE)的釣魚郵件攻擊行動

英國安全衛生執行署 (Health and Safety Executive，HSE) 屬於英國的公務部門，為各種專業人士和組織提供健康與安全解決方案。最近，賽門鐵克觀察到假冒衛安全衛生執行署指引 (尤其是 2022－2032 年的策略) 的網路釣魚活動，以竊取憑證。這些釣魚郵件通常偽裝成通知訊息，試圖引誘使用者開啟並點擊「Health and Safety Executive Strategy 2022-2032」。當受害者點擊電子郵件內容中的釣魚網址時，就會出現竊取憑證的網頁。

電子郵件標題：

- 郵件主旨： Prioritize Safety and Compliance-Schedule a Strategic Discussion(*優先處理安全與合規事宜-安排策略討論會)
- 寄件者："HSE RIDDOR"<造假的郵件帳號>

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。

2024/08/08

發現全新無檔案類型的勒索軟體：Cronus

據報導一種全新無檔案類型的勒索軟體被稱為 Cronus，最近涉入惡意軟體攻擊行動。使用者會被偽裝成 PayPal 收據的文件檔所誘騙。這些文件檔包含惡意的嵌入式 VBA 巨集，執行時會下載 PowerShell 載入器。載入器接著會使用反射 DLL 載入來部署勒索軟體 DLL，以逃避偵測。

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.Ps-Rd32!g1
- ACM.Word-Ps!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen16
- SONAR.MSOffice!g7

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!gen9
- CL.Downloader!gen205
- ISB.Downloader!gen464
- Ransom.HiddenTear
- 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。

2024/08/07

最近專門鎖定以色列～RHADAMANTHYS惡意竊密程式

RHADAMANTHYS 惡意竊密程式自 2013 年就已相當活躍，並以惡意軟體即服務 (Malware-as-a-Service) 的營運模式運作，最近開始以以色列使用者為目標，發送包含惡意 RAR 附件的希伯來語網路釣魚電子郵件。該 RAR 壓縮檔案偽裝成「Calcalist」或「Mako」(以色列兩家著名企業) 通知，解開後有三個元件--惡意執行檔案、DLL 檔案和支援檔案。執行後，RHADAMANTHYS 會使用反分析技術來避免偵測，並啟動多階段感染程序，達到在遭入侵系統上建立執行狀態。

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。

2024/08/07

暗度陳倉～SbaProxy惡意軟體以合法防毒軟體為掩護

最近的一份報告詳細說明威脅份子如何利用一種稱為「SbaProxy」的工具，偽裝成合法的防毒軟體，以便能夠透過 C&C 伺服器建立代理連線。該工具以惡意目的散佈，並採用多種格式，例如：DLL、EXE 和 PowerShell 腳本，由於其真實的外觀和先進的功能，使其難以被偵測到。

保安建議：不要在非原廠的網站上下載 (免費) 軟體。最常見的情境是感染惡意程式之後，急於解決問題時，往往搜尋到解毒／解密工具，就不分青紅皂白的下載使用。有很高機率是原來只是破皮，因為下載更危險的工具，導致截肢或歸西。

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.SbaProxy
- Trojan.Gen.MBT
- WS.Malware.1

2024/08/07

Lynx勒索軟體

Lynx 是另一款採取雙重勒索戰術的勒索軟體，最近幾週相當活躍，並在其網站上聲稱有多家公司成為受害者。他們宣稱有嚴格的政策 (盜亦有道)，嚴禁針對政府組織、醫院、非營利機構及其他對社會極其重要的機構組織。

一旦成功入侵，它們就會加密機器和滲出資料。被加密的檔案會被冠上 .LYNX 副檔名。勒索贖金支付說明文字檔 (README.txt) 會存放在不同的目錄中。它相當簡短，以下列兩句話開始："Your data is stolen and encrypted. Download TOR Browser to contact us.(您的資料已被盜取並已加密。下載 TOR 瀏覽器與我們聯絡)"。接著它會顯示一組隨機 ID，以及與他們對話聊天的洋蔥加密網站 (TOR) 的網址。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen14
- SONAR.RansomPlay!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

2024/08/07

惡意軟體攻擊行動利用secureserver.net網域部署銀行木馬程式

一個全新的銀行特洛伊木馬惡意軟體攻擊行動濫用 secureserver.net 網域來攻擊西班牙語和葡萄牙語地區。這種多階段攻擊從惡意網頁開始，指向一個包含經混淆過的 .hta 檔案壓縮檔。這個檔案會導向一個 JavaScript 有效酬載，在下載最後的 AutoIT 有效酬載之前，會執行多重 Anti-VM(反制沙箱的能力) 和 Anti-AV(規避防毒軟體偵測) 檢查。此有效酬載使用程序注手法載入，目的是竊取受害者系統中的銀行資訊和憑證，並將其滲出到 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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Wscr-CNPE!g1
- ACM.Wmip-Ps!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!aat171
- ISB.Downloader!gen66
- Scr.Malcode!gen
- Scr.Malcode!gen63
- Trojan Horse
- Web.Reputation.1
- 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。

2024/08/07

Chameleon全新木馬程式鎖定飯店業

據報導，全新的 Chameleon 行動銀行木馬程式鎖定餐飲業。加拿大一家國際連鎖餐廳的員工被偽裝成合法 CRM 應用程式的騙局誘騙。客戶關係管理 (CRM) 系統是整合式的資料驅動解決方案，用來管理、追蹤和儲存公司的客戶資訊。一旦安裝後，該應用程式會顯示偽造的 CRM 登入頁面，要求提供員工 ID，導致憑證被盜用，進而在未經授權的情況下存取企業銀行帳戶。此外，Chameleon 利用鍵盤側錄來收集其他敏感資訊，這些資訊後續可能會被濫用來進行進一步攻擊，或在地下論壇出售。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- WS.Malware.1

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

2024/08/07

Zola--最新的Proton勒索軟體後繼新變種

Zola 是 Proton 勒索軟體家族最近發現的最新變種。該勒索軟體以 C++ 撰寫，並採用多執行緒的加密程序。加密後，會被冠上 .zola 副檔名。Zola 也會嘗試加密任何網路裝置上的檔案 (如果有的話)。該惡意軟體具有從受感染的機器中刪除陰影複本以及在啟動過程中停用作業系統自動修復選項的功能。隨附的勒索贖金支付說明要求受害者透過提供的電子郵件地址與攻擊者聯繫，以獲得關於解鎖資料的進一步指示。

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-FlPst!g1
- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.C

2024/08/07

濫用雲端服務何其多?威脅份子的惡行惡狀

由於攻擊者已開始意識到合法雲端服務提供低調且低成本基礎架構的潛力，因此今年在攻擊中利用合法雲端服務的威脅份子數量明顯增加。相較於與攻擊者所架構控制的通訊架構，來自 Microsoft OneDrive 或 Google Drive 等知名、可信賴服務的流量可能較不易引起警覺。僅在過去幾週，賽門鐵克的威脅獵手團隊就發現三個使用雲端服務的間諜行為，並發現有證據顯示有更多工具正在開發中。目前利用雲端服務部署威脅的威脅份子數量顯示，間諜行動者顯然正在研究其他組織所建立的威脅，並模仿他們認為成功的技術。

請參閱我們的部落格：烏「雲」密布：惡意威脅份子如何濫用雲端服務。

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-Reg!g1
- ACM.Ps-RgPst!g1
- ACM.Rd32-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper
- SONAR.MalTraffic!gen1
- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Trojan Horse
- Trojan.Coinminer
- Trojan.Gogra
- Trojan.Grager
- Trojan.Gen.MBT
- Trojan.Moontag
- Trojan.Ondritols
- 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

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 Connecting to Cloud Storage
- 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。

2024/08/07

義大利爆發寄送夾帶Vidar惡意洩密程式的惡意郵件給認證過電子郵件帳號之攻擊行動

Vidar 惡意竊密程式被觀察到，最近針對義大利使用者的惡意垃圾郵件攻擊行動之有效酬載。該行動遞交給經認證電子郵件信箱的使用者，並透過電子郵件中連結傳送 JavaScript 下載程式。JavaScript 負責下載並執行 PowerShell 腳本，而 PowerShell 腳本則會導向最終的惡意有效酬載。

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.Wmip-Ps!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen569
- ISB.Suspexec!gen48
- Scr.Malcode!gen105

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。

2024/08/06
Mispadu(也稱為URSA)木馬惡意程式

Mispadu 惡意竊密程式 (也稱為 Ursa) 涉入最近在另一起針對西班牙文或葡萄牙文語系的電腦系統之惡意垃圾郵件攻擊行動。與之前行動類似，以逾期發票為主旨的垃圾郵件作為初始媒介，然後引誘使用者下載惡意 ZIP 檔案。這個壓縮檔包含一個 MSI 安裝檔，其中 VBScript 經過三層混淆。一旦解除混淆，腳本就會顯示 AutoIT Loader／Injector 並收集作業系統版本資訊。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan.Gen.NPE
- Web.Reputation.1
- 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。

2024/08/06
防護亮點：面對GitHub的惡意濫用

隨著世界變得越來越數位化，科技也變得更令人興奮和方便。軟體開發人員可以使用大量的線上工具來增進他們的技能、管理他們的程式碼以及形塑他們的想法。其中最受歡迎的應用程式之一是 **Git**，這是一套開放原始碼的版本控制軟體，可讓多位開發人員同時對各自的專案進行修改。開發人員也可以使用 **GitHub**，這是一個網頁型應用程式，可讓開發人員輕鬆地與其他開發人員分享檔案和進行協作。但不幸的是，這種便利性也有缺點。越來越多威脅份子濫用 GitHub 服務來寄生和散播垃圾郵件與惡意軟體。到目前為止，我們的防護公報中提到 GitHub 寄存或協助散播惡意軟體不下 44 次。平心而論，這類濫用絕非 GitHub 所獨有，但同樣令人擔心。

以下是一些濫用 GitHub 發動的攻擊鏈、惡意軟體原始碼/廣告、駭客工具，以及軟體和硬體漏洞的方式：

- **惡意軟體原始碼**：攻擊者可以在 GitHub 上傳並分享惡意軟體的原始碼，讓其他人可以存取，並將其用於惡意目的或進行修改。
- **惡意軟體散佈**：GitHub 儲存庫可用來寄存惡意檔案或腳本，然後透過網路釣魚電子郵件或其他方式散佈給受害者。
- **指揮與控制 (C&C)**：某些進階惡意軟體使用 GitHub 作為指揮與控制的平台，將與受感染機器的通訊隱藏在看似良性的資源庫活動中。

- **惡意軟體廣告**：GitHub 可以用來宣傳或展示惡意軟體的功能，將惡意軟體出售或與其他惡意行為者分享。
- **漏洞開採濫用**：GitHub 上公開分享的程式碼可能包含漏洞。攻擊者可以搜尋這些弱點，並利用它們進行廣泛的攻擊。
- **網路釣魚行動**：攻擊者可利用 GitHub 是知名且廣受信任的平台，在網路釣魚電子郵件中使用 GitHub 網頁，使其看起來像是合法的。

在本公告中，我們將介紹這些威脅所濫用的兩種常見攻擊媒介。

主題 1 攻擊媒介：惡意網頁

電子郵件被偽裝成政府組織的稅務相關通知，例如：美國國稅局 (Internal Revenue Service；縮寫 IRS) 和英國稅務海關總署 (His Majesty's Revenue and Customs，HMRC) 。

電子郵件本文要求收件人檢閱稅務相關文件，並在需要採取行動時作出回應。它們通常遵循以下模式：

- 電子郵件以正式的語氣撰寫，並在郵件內容中插入惡意的 GitHub 專案 (Project) 網頁。由於 GitHub 專案儲存庫頁面上的壓縮檔受密碼保護，因此電子郵件中也會提供簡短的密碼或 PIN。
- 點擊該網址會下載檔案，收件者會被提示輸入電子郵件內容中提供的密碼。加入這一步驟是為了向收件者保證一切都是合法的，沒有任何可疑的地方需要擔心。
- 在擷取壓縮檔內容之後，有效負載會有 .bat 到 .exe 不同的副檔名，以啟動一連串的事件，導致惡意感染和敏感資料的潛在損失。

攻擊鏈

- 電子郵件包含 github.com 專案內的網頁和密碼 → 重導向至專案頁面並包含密碼保護的壓縮檔 → DLL → .exe → 最終有效酬載

惡意網頁結構範例：

- hxxps[:]//github[.]com/[user_project]/[repo_name]/files/[file_id]/2023[.]COMPLETE[.]TAX[.]ORGANIZER[.]pdf[.]zip

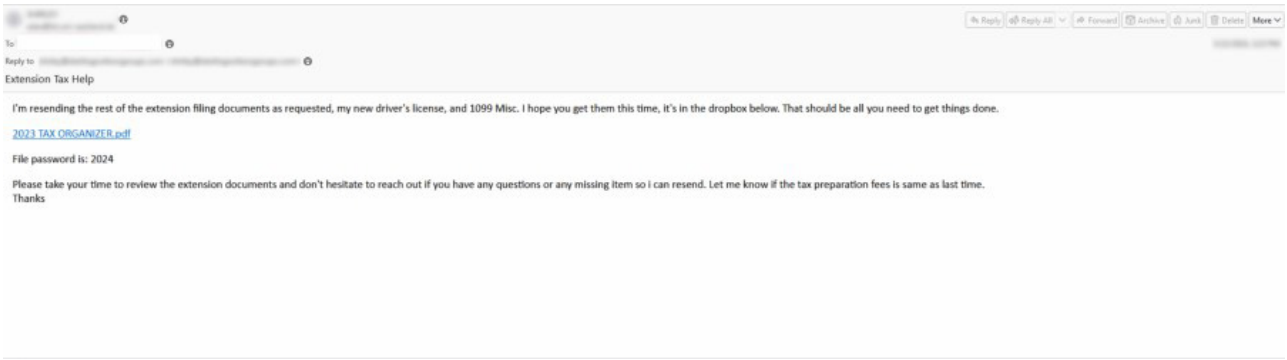

圖 1：內嵌 GitHub 專案儲存庫網址的電子郵件預覽

主題 2 攻擊媒介與手法： 附件

電子郵件被偽裝成有關法律團隊發出西班牙文的訴訟相關通知。

- 電子郵件本文部分的內容非常簡潔，使用正式的語氣和簡短的密碼，並有一個假冒的「.svg」檔案。

- 電子郵件收件人會被引誘下載「.pdf.svg」或「.docx.svg」副檔名檔案，其中包含內嵌的 github.com 專案儲存庫網址。
- github.com 專案儲存庫網址會為收件者提供受密碼保護的壓縮檔。
- 使用電子郵件中提供的密碼擷取出檔案後，有效籌載會有從 .bat 到 .exe 等各種副檔名，準備啟動一連串事件，導致惡意感染和敏感資料的潛在損失。

攻擊鏈

- 電子郵件包含附加的 .svg 檔案和密碼 → 重導向至 github.com 專案頁面，其中包含密碼保護的壓縮檔 → DLL → .exe → 最終有效酬載

圖 2：附有「.pdf.svg」副檔名檔案的電子郵件預覽

此類型的惡意垃圾郵件攻擊行動可能特別針對特定的電子郵件使用者群組，也可能針對較大的非目標群組，視攻擊行動特定目標而定。最終有效酬載各不相同，包括許多惡名昭章的威脅，例如：Remcos、AsyncRAT 和 Agent Tesla。

賽門鐵克防護機制

賽門鐵克的**郵件安全雲端服務 (Cloud Email Security Service) 和郵件安全閘道 (虛擬) 硬體裝置(Messaging Gateway)** 可發揮封鎖作用，這都歸功於一整套完整的先進技術，專門用於保護組織免受此類威脅。

- **反垃圾郵件過濾系統**：頻率近乎即時的各種網頁屬性的資料庫更新、檔案附件和其他電子郵件功能的系統，以跟上快速演進的電子郵件威脅環境變化。
- **模擬器和啟發式特徵**：我們的解決方案採用先進的模擬器和啟發式特徵碼來識別隱藏在電子郵件中的惡意元素。透過模擬程式碼執行和分析行為模式，我們可以在潛在威脅對組織造成影響之前，先行偵測並解除威脅。
- **透過 WebPulse 技術建立網頁信譽**：以雲端為基礎的架構，專以利用使用者導向行為的力量，並將使用者的回報轉換為全球網路情報和網路威脅情報。
- **連結追蹤**：賽門鐵克的專利技術，可掃描超連結，以判斷它們是否被用於垃圾郵件、網路釣魚或惡意目的。持續進行更新，以更好地識別 GitHub 儲存庫和網頁中的濫用情況。
- **賽門鐵克資料外洩防護(Data Loss Prevention)**：透過與我們的電子郵件安全解決方案無縫整合，協助對抗資料竊取情況。

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。
欲深入瞭解有關賽門鐵克基於雲的網路安全服務 (WebPulse) 的更多訊息，請點擊此處。

欲深入瞭解鐵克資料外洩防護 (DLP) 的更多訊息，請點擊此處。
可以透過以下網址回報垃圾郵件、惡意軟體或濫用 GitHub 服務：
https://docs.github.com/en/communities/maintaining-your-safety-on-github/reporting-abuse-or-spam

2024/08/06
XDSpy駭客集團針對俄羅斯和摩爾多瓦共和國的發動網路釣魚行動

據報導，XDSpy 駭客集團針對俄羅斯和摩爾多瓦的組織發動網路釣魚惡意軟體攻擊行動。攻擊鏈通常使用魚叉式網路釣魚電子郵件，其中的檔案附件包含與合約有關的誘餌，以部署被稱為 XDDown 的主要惡意軟體模組。此模組會安裝其他外掛程式，以收集系統資訊、密碼、本機檔案，並將資料滲出到攻擊者的 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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.B!100
- Heur.AdvML.C

2024/08/06
傳播Magniber勒索軟體的惡意活動激增

在真實網路情境上有發現最終會感染 Magniber 勒索軟體的活動激增。已知散佈此惡意軟體的攻擊者會利用各種傳播方式，包括惡意廣告、透過破解軟體安裝程式進行傳播或開採濫用已知漏洞等。Magniber 主要針對家庭使用者或小型企業。惡意軟體會加密使用者資料，並在被加密檔案冠上隨機的副檔名。隨附的勒索贖金支付說明要求受害者以比特幣支付贖款。

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.Rd32-RLsass!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.RansomMgnibr!g2
- SONAR.Ransomware!g19
- SONAR.Ransomware!g30
- SONAR.RansomGen!gen4
- SONAR.SuspLaunch!g193

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Magniber
- Ransom.Magniber!gen2
- Ransom.Magniber!g3
- 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.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：

- URL reputation: Browser navigation to known bad URL

2024/08/06

在OSX和Windows環境出現假冒成會議或生產力軟體的惡意軟體大肆傳播

有報導指出，惡意軟體偽裝成會議或生產力應用程式，持續散佈在真實網路情境上。最近一些實例包括偽裝成生產力應用程式 Wasper 或 Clusee 會議應用程式的攻擊。在此類攻擊行動中散佈的惡意竊密軟體會以 Windows 和 macOS 平台上的受害者為目標。惡意軟體的功能包括竊取各種機密資訊，例如：憑證、銀行詳細資訊、加密貨幣錢包、瀏覽器中儲存的資料等。其中一

個已發佈的有效酬載變種被發現屬於「StealC」惡意竊密軟體家族。

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：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan Horse
- 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。

2024/08/06

Swallowtail進階持續性滲透攻擊(APT)駭客集團大肆散布HeadLace後門程式

Palo Alto 最新研究報告指出，最近 HeadLace 後門散布攻擊行動是由 Swallowtail 進階持續性滲透攻擊 (APT) 駭客集團 (也被稱為 Fighting Ursa，APT28) 所為。攻擊者利用汽車銷售釣魚誘餌來散佈惡意有效酬載。攻擊鏈包括將使用者指向惡意 HTML 網站的自訂 URL、誘騙圖片和包含惡意二進位檔案的 .zip 檔案。此攻擊活動的有效酬載--HeadLace 後門會在濫用合法 Windows 電腦可執行檔時，側載到受害者電腦上。

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

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen523
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.Malscript

- W32.Ramnit.B
- Web.Reputation.3
- 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。

2024/08/05

IRATA手機木馬持續攻擊義大利

過去一年來，威脅份子持續使用一種名為 Irata 的 Android 遠端存取木馬程式，針對義大利和一些鄰近國家的行動使用者進行攻擊，這種木馬程式也具有竊取銀行資料的功能。

這段期間，他們作案手法並沒有太大的改變；他們主要利用包含重導網頁去下載惡意應用程式的惡意簡訊 (簡訊釣魚) 作為感染媒介。他們不斷轉換社交工程手法，賽門鐵克已觀察到多種義大利金融服務遭冒用。這顯示他們對當地環境的高度了解，讓行動使用者不疑有他而遭受攻擊。

最近幾週，我們觀察到一起全新的攻擊行動，攻擊者濫用偽造的 N26 Android APP (Certificato N26.apk) 作為誘餌。N26 是歐洲各地廣泛使用的知名行動銀行平台。被 Irata 入侵會導致消費者遭受財務損失、身份盜用和隱私權侵犯，而企業則會面臨資料外洩、財務損失和聲譽受損。

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：

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

2024/08/05

傳真與網路詐騙有關連嗎？這個憑證收集行動證明真的如此

賽門鐵克最近觀察到冒充傳真通知的網路釣魚行動。這些通知包含類似「Incoming Fax Delivered for user**@****.com」的標題，並指示使用者開啟所附 HTML 並輸入憑證，以檢視傳真。

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：

- Scr.Heuristic!gen13

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。

2024/08/04

Lumma惡意竊密程式透過社群媒體和AI相關的誘餌散播

據報導，有一起惡意廣告詐騙事件，網路犯罪分子劫持社交媒體頁面，推廣虛假的人工智慧照片編輯器，最終誘使用戶下載一種名為 Lumma 常見但平凡的惡意竊密程式。這種惡意軟體能夠竊取多種瀏覽器的登入憑證、Cookie和自動填寫表單資料，以及與加密貨幣錢包相關的瀏覽器擴充功能資料。它針對基於 Chrome 的雙因素和多因素身份驗證以及密碼管理的擴展程式。此外，它會透過檢查 AppData 中的預設錢包檔案位置，竊取與加密貨幣錢包應用程式相關的錢包和機密檔案。

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：

自適應防護技術(包含於SESC)：

- ACM.Rgasm-Lnch!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspOpen!gen11

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse

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。

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

2024/08/04

Trust(Crypto)加密貨幣錢包使用者遭受新一波網路釣魚攻擊

Trust Wallet 是一款加密貨幣錢包，提供使用者購買、出售、儲存、交換和管理加密貨幣等服務。最近，賽門鐵克發現有仿冒 Trust Wallet 服務的網路釣魚活動，誘使使用者開啟假冒的通知郵件。電子郵件內文內容提到，使用者需要驗證並啟用加密錢包，才能繼續使用 Trust 的服務，而不會暫停或中斷。用戶會收到偽裝成「驗證並啟動錢包」連結的釣魚網址--企圖引誘用戶打開並點擊設計用來竊取憑證的釣魚網址。

電子郵件主旨：

- 電子郵件主題：Verify And Activate Your Wallet (驗證並啟動您的錢包)
- 電子郵件寄件者：Trust Wallet <假冒的郵件位址>

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。

2024/08/04

BITSLOTH後門

BITSLOTH 是研究人員在拉丁美洲發現的 Windows 後門，利用背景智慧型傳送服務 (BITS) 進行命令與控制作業。根據報告，該程式已開發數年，可記錄按鍵、擷取畫面並收集大量資料。它使用進階的迴避技術，包括 shellcode 載入器和代理工具。

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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

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

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

2024/08/02

BlankBot行動銀行木馬程式，鎖定土耳其境內用戶

BlankBot 是一種全新的行動銀行特洛伊木馬，主要針對土耳其使用者。BlankBot 濫用 Android Accessibility 無障礙功能服務，從受感染的裝置取得完全控制權並收集資訊。其功能包括鍵盤記錄、簡訊內容轉發、螢幕錄影、收集應用程式清單等。透過 WebSocket 通訊與命令與控制 (C&C) 伺服器建立連線。該惡意軟體還採用反模擬技術。

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。

2024/08/02

NetSupport遠端存取木馬(RAT)攻擊行動

NetSupport Manager 已被威脅者加工成為武器用來執行惡意活動，並以遠端存取特洛伊木馬 (RAT) 運行。隨著時間的推移，已經發現各種不同的行動，每種行動都是在前一種行動的基礎上，嘗試透過多種混淆更新來發展規避技術。

最近的策略指出感染的 3 個階段：

1. 透過惡意廣告或被入侵的網站下載 JS。
2. 透過 JS 執行混淆的 PowerShell 指令碼以取得有效酬載之後執行並常註。
3. 結束，安裝 NetSupport Manager RAT 工具，並新增一些腳本以逃避偵測。

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-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- ISB.Downloader!gen40
- Trojan.Gen.NPE
- Trojan Horse
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

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: 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。

2024/08/02

AutoIT腳本工具被濫用於最新Konni遠端存取木馬(RAT)的散播

在最近觀察到的 Konni 遠端存取木馬 (RAT) 散播行動中有發現濫用 AutoIT 腳本工具來逃避偵測。攻擊鏈包括使用 .zip 壓縮檔中的 .LNK 檔案。.lnk 捷徑檔案通常以雙重副檔名來偽裝成文件檔，例如：「.hwp.lnk」。捷徑檔案中存在預先寫好的 Powershell 指令碼，可在執行檔案時向受害者顯示成偽裝文件，同時在背景中繼續執行惡意程式。此惡意軟體具有從受攻擊的端點擷取機密資料，以及執行從 C&C 伺服器接收遠端指令的功能。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Schtsk!g

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Heur.AdvML.A!500
- 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。

2024/08/02

觀察到Neshuta惡意軟體的活動激增

上個月賽門鐵克發現 Neshuta (也稱為 Neshta) 惡意軟體家族的活動激增。Neshuta 是一種較舊的檔案感染型之惡意程式，早在 2005 年就已出現在威脅領域。它的主要功能是在可執行檔案中預先加入病毒碼，並收集基本的系統資訊。該惡意軟體還具備在受感染端點上常駐的功能

。多年來，Neshuta 也開始越來越被用作惡意酬載的注入器--導致感染其他惡意軟體變種，包括 Hardbit 等勒索軟體。

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：

自適應防護技術(包含於SESC)：

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

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.6
- Trojan.Gen.MBT
- W32.Neshuta
- 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

2024/08/02

Grayfly(也稱為APT41)駭客組織最近在針對台灣的攻擊中部署ShadowPad和Cobalt Strike

根據 Cisco Talos 資安研究人員的報告，最近在台灣觀察到 Grayfly 駭客組織 (也稱為 APT41) 散佈惡意軟體的攻擊行動中，部署了 ShadowPad 惡意軟體和滲透測試工具 Cobalt Strike beacons。據報導，攻擊者利用舊版且易受攻擊的 Microsoft Office 輸入法 (IME) 檔案 (imecmnt.exe) 來執行第二階段載入程式和。ShadowPad 是具有後門功能的模組化惡意軟體，也是知名 PlugX 惡意軟體的後繼變種。在這次討論的行動中，還部署自訂版本的 Cobalt Strike 載入器。這個變種是以 Go 程式語言寫成，並基於一個名為「CS-Avoid-Killing」反防毒軟體的後門，先前已在各種駭客論壇上打過廣告。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Backdoor.Shadowpad
- PasswordRevealer
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- 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。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。