保安資訊--本周(台灣時間2023/10/20)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 66 萬 1,200 台受保護端點上總共阻止了 8,170 萬次攻擊。這些攻擊中有 86.1% 在感染階段前就被有效阻止：**(2023/10/16)**

- 在**11萬8,300**台端點上，阻止了**3,250**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**19萬6,900**台端點上，阻止了**1,590**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬4,300**台**Windows**伺服主機上，阻止了**1,520**萬次攻擊。
- 在**6萬9,500**台端點上，阻止了**270**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,400**台端點上，阻止了**120**萬次嘗試掃描在**CMS**漏洞。
- 在**5萬5,300**台端點上，阻止了**160**萬次嘗試利用的應用程式漏洞。
- 在**24萬5,500**台端點上，阻止了**500**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**7,100**台端點上，阻止了**210**萬次加密貨幣挖礦攻擊。
- 在**12萬8,000**台端點上，阻止了**940**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**937**台端點上，阻止了**6萬2,300**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。

2023/10/19

CVE-2023-38545 Curl中的堆積緩衝區溢位(Heap Buffer Overflow)漏洞

CVE-2023-38545 是最近在 Curl 指令行工具和 libcurl 函式庫發現高嚴重堆疊緩衝區記憶體溢位漏洞。它影響透過使用 libcurl 程式庫 SOCKS5 代理連接及嘗試解析長主機名稱的應用程式。雖然要成功開採利用該漏洞有幾個必要條件，但它有可能導致遠端執行程式碼 (RCE)。新的 curl 8.4.0 修正版本已發佈，以解決此漏洞。以下為保安補充：curl 是一個廣泛用於命令行界面的工具，用於在各種網路協議之間進行數據傳輸。它的名稱來自『Client for URLs』(URL 的客戶端) 縮寫。'curl' 可以在不同的作業系統中使用，包括 Linux、macOS、Windows 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：

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: Curl Heap Overflow CVE-2023-38545

基於安全強化政策(適用於使用DCS)：

- DCS 內建的 sym_unix_protection_sbp 和 sym_win_hardened_sbp 安全政策，即能完全提供針對 curl 的 CVE-2023-38545 漏洞多重零時差保護。
  - DCS UNIX 強化防護政策可防止 Linux／UNIX 系統上的特權應用程式和使用者任意使用 curl 工具。
  - Windows 和 UNIX 預設的強化沙箱和應用程式自訂沙箱，可保護底層作業系統資源不受使用 libcurl 建構的應用程式影響，並防止攻擊者使用多種技術實現持續性和任意代碼執行。
  - 此外，DCS 基礎偵測政策會對系統篡改和可疑使用者活動 (如登錄嘗試失敗) 發出警報。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/10/19

以員工福利報告和薪資修訂為幌子的全新網路釣魚活動

威脅者繼續為網路釣魚電子郵件範本增添創意，這次涉及是員工福利。在最近一次網路釣魚活動中，偽裝成福利報告或員工薪資修改通知的電子郵件被發送給收件人，並附上包含網路釣魚網址 (URL) 的偽造文件。電子郵件主旨包含電子郵件地址部分和時間戳記。這樣做更富人情味，也較容易引誘使用者打開電子郵件。電子郵件內文內容刻意簡短，在某些情況下，內文內容會嵌入圖片中。

- [日][月][年][時間][電子郵件地址]的員工薪資修正／福利報告
- [日][月][年][時間]福利預先審查已批准：所有『薪資』修正案（已修訂）

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。

2023/10/19

與伊朗有關聯的Crambus駭客組織對中東某國政府進行長達八個月的入侵

博通公司旗下的企業安全部門：賽門鐵克威脅獵手團隊觀察到，中東某國政府遭到長達八個月的入侵。該行動是由與伊朗有關的進階持續威脅 (APT) 組織：Crambus(又名 OilRig、MuddyWater、APT34) 發起。這次攻擊包括惡意軟體傳送、情報收集、以檔案和憑證形式進行的資料竊取，以及為便於傳播而進行的系統修改。

在我們的部落格文章有更詳細的資訊可供參閱：Crambus 駭客組織鎖定中東政府機構進行的全新網路攻擊行動。

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：

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：

- Backdoor.PowerExchange
- Backdoor.Tokel
- Backdoor.Trojan
- Infostealer.Clipog
- Spyware.Keylogger
- Trojan Horse
- Trojan.Dirps
- WS.Malware.1
- 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.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。

2023/10/19

Xret勒索軟體

我們發現一款名為 Xret 的勒索軟體。加密成功後，它會在加密檔中冠上 .Xret 的副檔名。留在機器上的勒索贖金支付說明檔 (# XRET #.txt) 會通知受害者透過「Proton Mail」信箱服務或 WhatsApp 號碼與他們聯繫。攻擊者還在贖金支付說明提到，他們已經加密並竊取檔案，意在進一步向受害者施壓。此外，他們還表示自己沒有政治動機，只是為了錢。

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.SuspBeh!gen625

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1

基於機器學習的防禦技術：

- Heur.AdvML.B

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，當然能讓 Xret 勒索軟體攻擊者，無功而返。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/10/18

MesaCorp勒索軟體

MesaCorp勒索軟體 (源於 Chaos 的變種) 已經讓土耳其和其他國家傳出災情，它以單機而非企業網路環境為目標，勒索價值 2 美元的門羅幣，在撰寫本文時相當於 299 美元。被加密的檔會被冠上 .MesaCorp 副檔名，勒索贖金支付說明檔 (用英語和土耳其語書寫) 會被存到不同的位置。並將桌面背景替換為包含勒索贖金支付說明的圖片。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen625

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.HiddenTear!g1

基於機器學習的防禦技術：

- Heur.AdvML.B

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，當然能讓 MesaCorp 勒索軟體攻擊者，落荒而逃。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/10/18

Earth Grass(*地球草)勒索軟體

據觀察，又有一個勒索軟體攻擊者到處點火，他們將自己的勒索軟體冒充成 Windows OneDrive 安裝程式，並自稱為『Earth Grass (*地球草)』。如果使用者上當受騙下載假冒的安裝程式並執行它，他們的檔案就會被加密並被冠上 .34r7hGr455 副檔名。它還會留下一個勒索贖金支付說明檔 (檔名：Read ME (Decryptor).txt)，勒索價值 200 美元的門羅幣 (XMR)。目前，該程式並未採用邪惡的雙重勒索策略，也不會在環境中橫向移動以加密更多機器。

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.SuspBeh!gen625

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Zombie

基於機器學習的防禦技術：

- Heur.AdvML.B

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，當然能讓 Earth Grass (*地球草) 勒索軟體攻擊者，落荒而逃。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2023/10/18

安卓手機行動平臺出現的全新遠端存取木馬(RAT)：Rusty Droid

Rusty Droid 是一款針對安卓手機行動平臺的全新遠端存取木馬(RAT)。該惡意軟體偽裝成谷歌 Chrome 瀏覽器手機 APP 的 .APK (Android Package) 安裝包。該惡意軟體具有多種功能，包括發送／接收簡訊、攔截 Gmail 電子郵件、讀取連絡人清單、鍵盤側錄、撥打高資費電話和資料注入。Rusty Droid 會濫用遭入侵裝置上的無障礙服務 (Accessibility Service) 來執行惡意操作。收集到的資料會被外滲到攻擊者所操控的 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：

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
- Android.Reputation.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。

2023/10/17

網域名稱誤植蟑螂(Typo-squatters)濫用美國郵政署(USPS)域名的網路釣魚行動

賽門鐵克最近觀察到多個濫用美國郵政署 (USPS) 的網域名稱誤植蟑螂 (在 48 小時內註冊 341 個獨特的域名)，這些域名被濫用於助長簡訊釣魚行動，企圖借此獲取敏感資訊。攻擊者將向手機用戶發送自稱來自 USPS 的惡意簡訊，告知他們投遞問題。惡意重導向只有在透過瀏覽器 APP 開啟的網址 (URL) 時才會起作用。如果用戶使用非 APP 瀏覽器開啟 URL，他們將被重定向到真正的 USPS 網站。

- 簡訊示例：USPS 包裹已到達倉庫，由於位址資訊不完整而無法投遞。hxxps[:]//usps-adba[.]top/（請回復 Y，然後退出簡訊，再次打開簡訊啟動連結，或將連結複製到 Safari 瀏覽器打開)。美國郵政團隊祝您有美好的一天 (The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours. hxxps[:]//usps-adba[.]top/ (Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it). The US Postal team wishes you a wonderful day)

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：

Symantec Endpoint Protection Mobile (賽門鐵克端點安全手機／行動版) 能夠分析簡訊中內嵌的鏈接。它根據賽門鐵克全球情資網路 (GIN) 中的威脅情報偵測簡訊中內嵌的網址 (URL)，並在鏈接有疑慮時向使用者發出警告，從而保護使用者免受簡訊類型的網路釣魚的攻擊。GIN 中的 WebPulse 網頁安全情資生態系統，已於第一時間完整收納此次行動中被濫用的近似美國郵政署 (USPS) 的網域名稱。

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)：

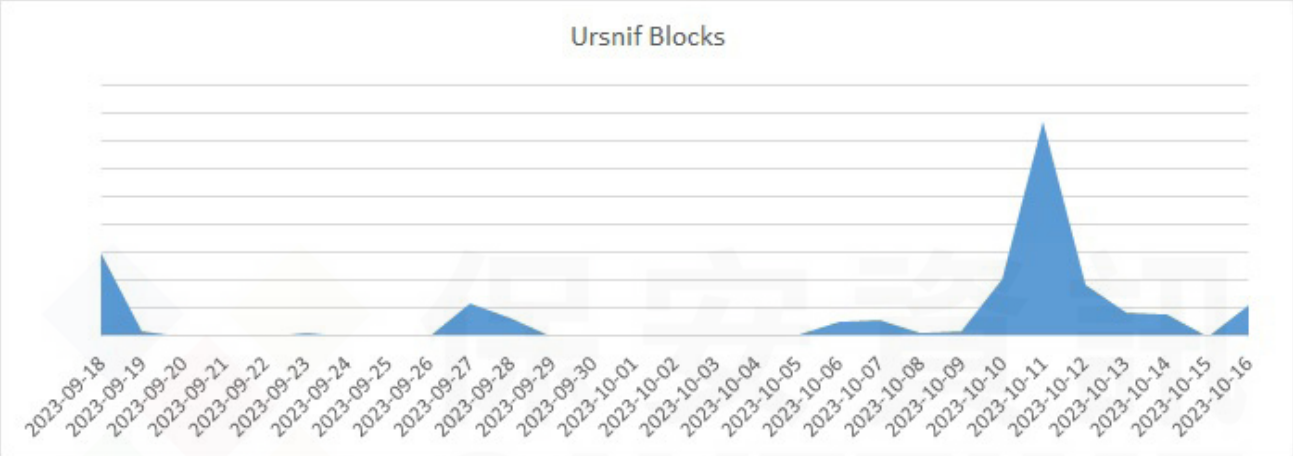
被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2023/10/17

防護亮點：Ursnif銀行金融木馬家族，冒充義大利國稅局

Ursnif (又名 Gozi、Snifula) 是一個著名的銀行金融木馬家族，已有 15 年以上的歷史。在此期間，它的原始程式碼曾多次公開洩露，因此產生了許多不同的變種。Ursnif 主要透過惡意垃圾郵件傳播，目的在從遭入侵染系統中竊取登錄憑證、雙因子驗證碼、銀行詳細資訊和其他機密資料。

最近觀察到傳播 Ursnif 的行動，主要針對義大利的金融機構冒充稅務局。全然不是意外，因為每年這個時候都是提交各種稅務相關表格的最後期限。



使用者會收到一封電子郵件，通知他們『報稅金額不對』，並說明需要立即採取行動。用戶被告知，他們可以直接瀏覽『Agenzia Entrate』(國內稅收署) 網站，或者瀏覽電子郵件附件中的檔案，該檔案的副檔名為 .URL，受密碼保護，密碼在電子郵件本文中提供。

電子郵件中的連結旨在使用 SMB 協定瀏覽網頁伺服器上的一個目錄，該目錄隨後將連接到另一個網址，用來下載包含惡意 CPL(控制台) 檔的 .ZIP 壓縮檔，進而觸發感染鏈的開始。

該郵件的主旨經常是如下的內容：

- Comitato di osservazione dell'anagrafe tributaria
- Commissione di monitoraggio del registro tributario
- Gruppo di controllo del registro tributario
- Comitato di monitoraggio dell'anagrafe tributaria
- Comitato per l'osservanza dell'anagrafe tributaria
- Organismo di supervisione sull'anagrafe tributaria

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 多重防護技術能在第一時間就偵測到該惡意程式及有效對應**零時差**攻擊的防護機制及其威脅名稱：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Downloader
- Trojan Horse
- Trojan.Mallnk

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。

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
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。
欲深入瞭解有關賽門鐵克基於雲的網絡安全服務 (WebPulse) 的更多訊息，請點擊此處。

2023/10/17

Atlassian的DevOps協作平臺：Confluence存在CVE-2023-22515的無效存取控制漏洞，並在真實網路情境被開採利用

CVE-2023-22515 是最近披露的一個影響 DevOps 協作平臺：Atlassian Confluence Data Center 和 Server 某些版本的嚴重等級 (CVSS 評分：10.0) 的提權漏洞。如果開採利用該漏洞，遠端攻擊者可透過建立未經授權的 Confluence 管理員帳戶來存取 Confluence 實例。據報導，該漏洞已在真實網路情境被開採利用，對目標網路進行初始存取攻擊。至少從 9 月中旬開始，Storm-0062(又稱 DarkShadow 或 Oro0lxy) 就是利用該漏洞進行攻擊的駭客組織之一。原廠 Atlassian 已經發佈修補程式，以解決 8.3.3、8.4.3、8.5.2 或更新版本中的此一漏洞。

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：

- Attack: Confluence Broken Access Control Vulnerability CVE-2023-22515

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。

2023/10/17

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 1.49 萬個受保護端點上阻止了總計 710 萬次攻擊。

- 使用網頁信譽情資，在 1.296 萬個端點上阻止了 610 萬次攻擊。
- 攔截了 34.3K 個端點上的 725.6K 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 15.3K 個端點上攔截了 183.8K 次瀏覽器通知詐騙攻擊。
- 在 867 個端點上攔截了 80.6K 次攻擊，這些攻擊利用了被入侵操控的網站上的惡意腳本注入。
- 在 1.8K 個端點上阻止了 3.9K 次技術支援詐騙攻擊。
- 在 282 個端點上阻止了 658 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。

2023/10/17

新版Lumma Stealer竊密程式，透過Discord傳播

Lumma Stealer 竊密程式是用 C 語言撰寫，至少從 2022 年開始就存在於威脅環境中。最近，人們在真實網路情境發現一種利用 Discord 內容交付網路 (CDN) 傳播這種惡意軟體的新行動。一旦感染機器，Lumma 就會試圖竊取存儲在系統瀏覽器中的資料以及任何存在的加密貨幣錢包。該惡意軟體繼續在地下論壇上銷售，並隨著最新版本的不斷發展而持續演化，增加在受感染端點上載入額外任意有效籌載的新功能。

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：

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

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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: Infostealer LummaC2 Activity
- System Infected: Infostealer LummaC2 Activity 02

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。

2023/10/16

TA577駭客組織發動的惡意郵件攻擊行動持續惡化--傳播DarkGate

DarkGate 載入器於 2018 年首次被觀察到，在執法部門取締 Qakbot 後，過去幾週的流行度有所上升。很有可能是由於這次行動，自 9 月以來，名為 TA577 駭客組織 (曾與 Qakbot 有聯盟夥伴關係) 在繼續傳播 Pikabot 和 IcedID 的同時，也開始透過其惡意電子郵件行動傳播 DarkGate。

雖然 DarkGate 主要用作載入器，但它還具有 HVNC(隱藏虛擬網路連線) 模組、鍵盤側錄功能和資訊竊取功能。在過去幾周裡，賽門鐵克觀察到多個 TA577 攻擊鏈透過其工具和技術不斷輪轉，如下所述。

- 9月21日：
  - Email > ZIP > LNK > CURL > VBS > AutoIT > EXE (DarkGate)
- 9月23日：
  - Email > URL > ZIP > LNK > CURL > VBS > AutoIT > EXE (DarkGate)
- 9月25日：
  - Email > PDF > URL > XLL > HTA > CURL > VBS > MSI > AutoIT > EXE (DarkGate)
  - Email > PDF > URL > XLL > HTA > CURL > VBS > AutoIT > EXE (DarkGate)
- 9月26日：
  - Email > PDF > URL > XLL > CURL > DLL (IcedID)
  - Email > PDF > URL > ZIP (Password Protected) > LNK > CURL > VBS/MSI > AutoIT > EXE (DarkGate)
- 9月28日：
  - Email > URL > ZIP (Password Protected) > LNK > CURL > DLL (Pikabot)
  - Email > URL > ZIP (Password Protected) > LNK > CURL > DLL (IcedID)
- 10月02日：
  - Email > URL > Zip (Password Protected) > LNK > CUR > VBS > CMD > CURL > AUTOIT > EXE (DarkGate)
  - Email > PDF > URL > Zip (Password Protected) > LNK > CUR > VBS > CMD > CURL > AUTOIT > EXE (DarkGate)
- 10月03日：
  - Email > PDF > TDS-404 > URL > XLL > HTA > CMD > CURL > DLL (DarkGate)

- 10月04日：
  - Email > URL > ZIP > LNK > Regsvr32 (*.sct) > Rundll32 > DLL (Pikabot)
  - Email > PDF > URL > ZIP > VBS > CMD > CURL > DLL (DarkGate)
  - Email > PDF > URL > ZIP > JS > PS(on memory) > DLL
- 10月05日：
  - Email > HTML > ZIP > PEEXE (Bumblebee)
  - Email > URL > ZIP > JS > PEDLL (PikaBot)
- 10月09日：
  - Email > URL > ZIP > MSI > AUTOIT > PEEXE (DarkGate)
- 10月10日：
  - Email > URL > JS > CURL > PEDLL (Bumblebee)
  - Email URL > ZIP > MSI > KeyScramblerIE > Shellcode > CMD > CURL > AUTOIT (DarkGate)
  - Email > PDF > URL > ZIP > MSI > KeyScramblerIE > Shellcode > CMD > CURL > AUTOIT (DarkGate)
  - Email > URL > ZIP > VBS > AUTOIT (DarkGate)
- 10月11日：
  - Email > PDF > URL > ZIP > MSI > AUTOIT (DarkGate)
  - Email > PDF >URL > ZIP > VBS > AUTOIT (DarkGate)
- 10月13日：
  - Email > MS TEAMS > URL > ZIP > LNK > PS > AUTOIT (DarkGate)
  - Email > PDF > URL > ZIP > MSI > AUTOIT (DarkGate)
  - Email > PDF >URL > ZIP > VBS > AUTOIT (DarkGate)

透過密切跟蹤 TA577 的活動及其不斷演變的攻擊鏈，賽門鐵克確保我們的安全措施得到持續更新和改進。

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.Heur.Dropper

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- ISB.Downloader!gen68
- ISB.Dropper!gen1
- ISB.Houdini!gen7
- Js.Downloader
- Memscan.SuspLoad!g1
- Trojan.Gen.MBT

- Trojan Horse
- Trojan.Darkgate
- Trojan.Darkgate!gen1
- Trojan.Darkgate!gen2
- VBS.Downloader.Trojan
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.B
- 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: Malicious File Download Request 3
- 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。

2023/10/13

SeroXen遠端存取木馬(RAT)，透過檔名輸入錯誤或記憶錯誤的NuGet套裝軟體平台傳播

SeroXen 遠端存取木馬(RAT)，最早出現在 2022 年的威脅環境中。從那時起，該惡意軟體就作為一種即用型工具在網上進行宣傳和銷售，無需任何高深術訣竅即可輕鬆操控。據信，SeroXen 部分源於惡意名昭彰 Quasar 遠端存取木馬 (RAT)，一旦安裝到目標主機上，攻擊者就可以遠端控制和執行命令。最近觀察到的傳播 SeroXen RAT 的行動是透過輸入錯誤或記憶錯誤的人的漏洞，將惡意二進位檔案偽裝在開源軟體套件管理系統平台 NuGet 上架的檔名相似或相近的套裝軟體中。

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