保安資訊--本周(台灣時間2023/08/04)
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 68 萬 1,800 台受保護端點上總共阻止了 8,240 萬次攻擊。這些攻擊中有 93.3% 在感染階段前就被有效阻止：**(2023/07/30)**

- 在**13萬5,500**台端點上，阻止了**3,090**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**22萬8,200**台端點上，阻止了**1,750**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**4萬9,400**台**Windows**伺服主機上，阻止了**1,480**萬次攻擊。
- 在**9萬800**台端點上，阻止了**250**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,100**台端點上，阻止了**94萬4,600**次嘗試掃描在**CMS**漏洞。
- 在**6萬9,200**台端點上，阻止了**150**萬次嘗試利用的應用程式漏洞。
- 在**23萬4,500**台端點上，阻止了**540**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**9,900**台端點上，阻止了**190**萬次加密貨幣挖礦攻擊。
- 在**13萬8,800**台端點上，阻止了**970**萬次向惡意軟體**C&C**連線的嘗試。
- 在**2,200**台端點上，阻止了**7萬6,000**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。

2023/08/03

網路上發現的新版NodeStealer竊密惡意軟體2.0

新版的 NodeStealer 竊密惡意軟體 2.0，已經透過網路釣魚行動在網路上傳播。該惡意軟體的主要功能是竊取瀏覽器 cookie，以接管 Facebook 企業帳戶。發現的新版 NodeStealer 惡意軟體 2.0 是用 Python 程式語言所編寫，具有竊取加密貨幣和下載其他任意有效籌載的額外功能。NodeStealer 下載的有效籌載，包括 BitRAT、HVNC RAT 和 Xworm。

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.2
- 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.A
- Heur.AdvML.B

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。

2023/08/02

CyberCartel駭客組織發起的惡意軟體傳播行動

CyberCartel 是一個至少自 2012 年以來主要活躍在墨西哥和其他拉丁美洲國家的駭客組織。該駭客組織高度依賴惡意軟體即服務 (Maas) 營運商所提供的各種多元惡意軟體。該駭客組織所發起的最新惡意攻擊行動一直利用惡意廣告作為惡意軟體傳播的主要手段。攻擊者一直在部署具有各種功能的惡意籌載，例如：資訊竊取、銀行金融資料盜竊、螢幕截圖、剪貼簿覆蓋、惡意重導向、流量攔截等。

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：

- 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.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE.C
- 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

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 676
- System Infected: Trojan.Backdoor Activity 704
- 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。

2023/08/02

遭入侵的WebDAV伺服器，被利用來傳播XWorm惡意軟體

賽門鐵克監控到利用遭入侵的 WebDAV 伺服器來傳播 XWorm 惡意軟體的全新攻擊行動。攻擊鏈從透過惡意垃圾郵件散佈的 .LNK 檔案開始。.LNK 檔案執行後，就會執行遠端 WebDAV 伺服器上託管的惡意 PowerShell 程式碼，該程式碼又會下載包含 BATloader 惡意軟體二進位檔案的 .zip 壓縮檔。載入程序的功能是將 XWorm 注入遭入侵的端點上正在執行的程序中。被注入的 XWorm 有效籌載的功能，包括用戶資料盜竊、加密錢包位址置換、發動 DDoS 攻擊或下載其他有效籌載。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.BatCloak!gen1
- SONAR.SuspBeh!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn14
- Trojan Horse

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

基於機器學習的防禦技術：

- Heur.AdvML.B

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。

2023/08/01

SpyNote間諜軟體，正鎖定銀行機構

安卓平台上知名的手機行動裝置間諜軟體：SpyNote 自 2016 年以來一直在傳播，威脅研究人員最近發現另一個攻擊行動。這次攻擊是直接鎖定歐洲地區的銀行機構，透過簡訊釣魚（簡訊網路釣魚）發動攻擊。受害者被要求下載並安裝『認證過的新版銀行APP』，然後隨後的訊息會指示用戶啟動 TeamViewer 程序，這實際上是允許歹徒操控受害者裝置的第一步。

SpyNote 的功能列表：

- 鍵盤側錄
- 簡訊劫持並繞過雙因素認證 (2FA) 機制
- C&C 連線
- 螢幕錄製和規避安全軟體檢查

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：

- 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

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。

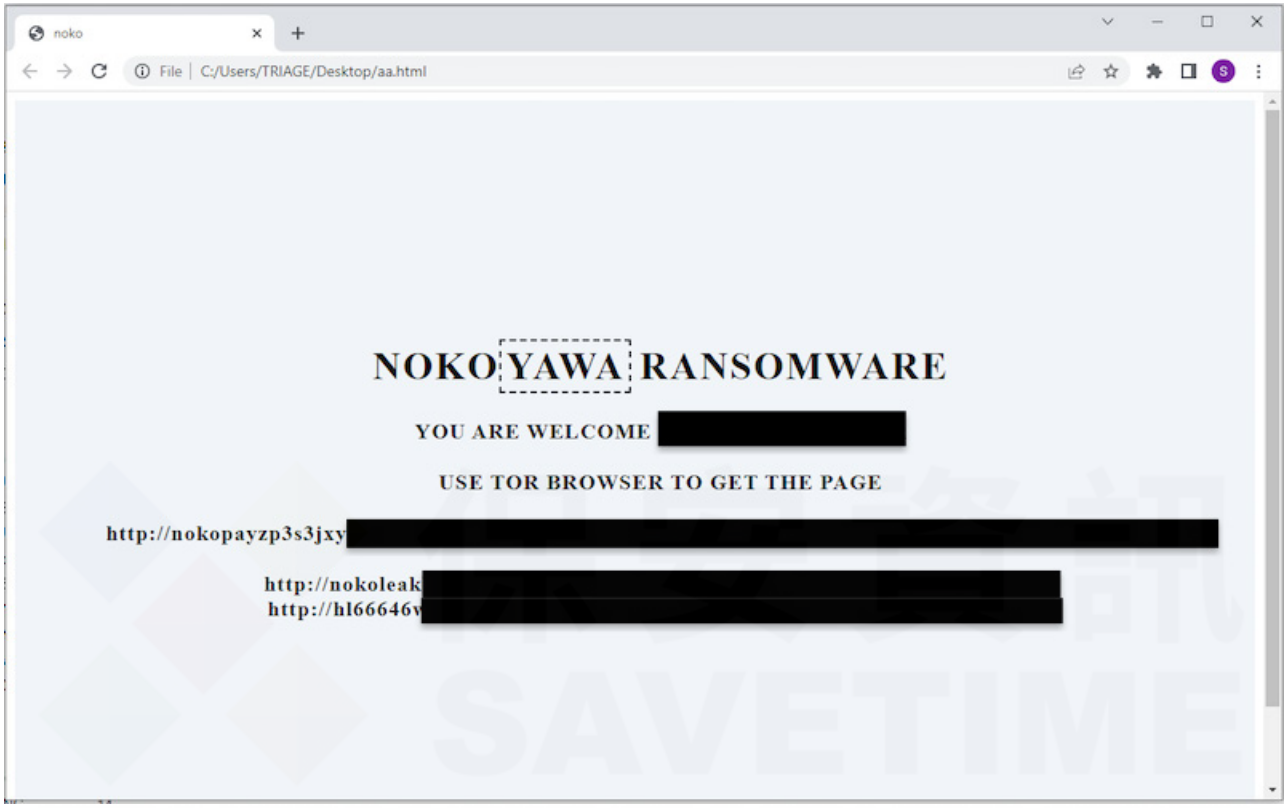
2023/08/01

防護亮點：Nokoyawa勒索軟體

Nokoyawa 勒索軟體自 2022 年初以來就非常活躍，並因開採利用存在於 Windows 系統的 Common Log File System（CLFS）服務的漏洞 CVE-2023-28252 而引起關注。隨著時間的推移，Nokoyawa 的作者對勒索軟體進行大改版，將其轉換為 Rust 語言。

與其他讓人聞風喪膽的勒索軟體攻擊者一樣，作者在他們的攻擊鏈中採用一系列策略、技術和程序 (TTPs)。2022 年底，發現他們利用 IcedID 的受害者來獲得初始存取權限。

成功入侵後，被加密檔案將被冠上 .NOKONOKO 副檔名，並在電腦上存放勒索贖金支付說明檔（最新版本中為 NOKONOKO-readme.txt 或 NOKONOKO-readme.html）。下面是一個例子：



Nokoyawa 勒索軟體的主要目標是企業和組織，特別是醫療保健、金融服務、政府和製造業等行業。鎖定這些機構通常是因為它們擁有敏感資料、關鍵作業以及可能支付大量贖金的意願。報告顯示，贖金通常平均價值約為 20 萬美元的比特幣。

在Nokoyawa攻擊鏈中所採用的 TTPs 依MITRE 所分類的包括以下內容：

- Command and Scripting Interpreter: Windows Command Shell [T1059.003]
- Windows Management Instrumentation [T1047]
- Data Encrypted for Impact [T1486]
- Impair Defenses: Disable or Modify Tools Defacement [T1491]
- Defacement [T1491]

賽門鐵克提供的單一解決方案內建多層級防護技術，個別技術多能在第一時間就具備**零時差**防護的能力並有明確的定義，謹就不同防護技術說明如下：

基於行為偵測技術(SONAR)的防護：

- SONAR.WMIC!gen12
- SONAR.RansomPlay!gen1
- SONAR.Ransom!gen35
- SONAR.Ransomware!g13

- MEMSCAN.Ransom!gen1
- MEMSCAN.Ransom!gen8
- SONAR.SuspLaunch!g258
- ACM.Wmip-Ps!g1
- MEMSCAN.Ransom!gen2
- SONAR.Ransom!gen98
- SONAR.RansomGen!gen3
- SONAR.RansomNoko!g3

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訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Ransomwares/Nokoyawa.

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Nokoyawa

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)：

賽門鐵克重要主機防護系統：DCS～Data Center Security 內建的預設強化政策，即能提供針對未知威脅的零時差防護，包括以前未見過的勒索軟體變種和相關行為。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

欲深入瞭解更多有關於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。

2023/08/01

惡意軟體利用已編譯的HTML說明檔案(CHM)～最近針對韓國用戶的攻擊行動中被廣為散播

根據最近發布的一份報告，利用已編譯的 HTML 說明檔案 (Microsoft Compiled HTML Help, CHM) 的惡意攻擊行動，已被發現冒充韓國金融機構和保險公司的通訊指南。這些詐騙指南涵蓋『信用卡額度』、『保險費退回結果』和『銀行契約』等主題。如果受害者被誘騙執行惡意 CHM 檔案，他們會在不知不覺中讓惡意軟體感染自己的電腦，這些惡意軟體可用於竊取用戶憑證和個人資料等。

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：

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：

- Downloader
- Infostealer.Eynice

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。

2023/07/31

Bahamut高階駭客組織，鎖定Android手機用戶

安全研究人員發現針對南亞個人的手機行動裝置攻擊行動。被稱為『CoverIm』的 Android 惡意軟體是偽裝成 SafeChat 的聊天 APP，並透過 WhatsApp 傳播。該惡意軟體能夠利用間諜軟體感染受害者的設備，竊取通話記錄、簡訊和 GPS 位置。CoverIm 還可以從 Telegram、Signal、WhatsApp、Viber 和 Facebook Messenger 等應用程式的情境中竊取資料。

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：

- 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

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。

2023/07/31

冒充Ozow和PayFast這兩家金融科技公司的網路釣魚行動在南非造成嚴重災情

手機行動金融服務在南非大受歡迎，用戶數更是屢破紀錄。此熱潮也讓南非的金融服務更多元，造福更多無法由傳統金融服務的民眾。然而，網路銀行的興起也吸引網路犯罪分子，他們試圖利用潛在的漏洞謀取利益。

最近，賽門鐵克觀察到大量簡訊網路釣魚（也稱為簡訊釣魚）企圖冒充 Ozow 和 PayFast 這兩家提供線上支付解決方案的南非著名金融科技公司。這些訊息包括模仿金融科技的惡意網站的短網址，提示用戶選擇他們的銀行，然後洩露敏感資料。這可能會導致身份被盜、經濟損失，並可能導致進一步的詐騙。

觀察到的惡意簡訊範例（按原樣--包括拼寫錯誤）：

- Ozow Payment. Confirm incoming deposit. Please click this hxxps://dik[.]si/Wepay0zownow to approve deposit to your credit/cheque account from SARS retuns.
- Ozow Payment. Confirm your deposit. Please visit https hxxps://shp[.]zone/ljiE to complete deposit to your credit/cheque account; 26/07/2023.
- PayFast:A payment has been sent to your Debit/Credit card vai SARS. Tap LINK hxxps://dik[.]si/Payfastnow02 to recieve payment into your Account, T&C's Apply.

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。

2023/07/31

全新的CherryBlos手機行動裝置惡意軟體

CherryBlos 是一種全新的手機行動裝置惡意軟體，可以竊取加密貨幣錢包的憑證或在加密交易期間替換錢包位址。該惡意軟體透過熱門社交網路入口上的貼文進行傳播，其中包含將用戶重導向到傳播惡意 APP 的網路釣魚網站的廣告。CherryBlos 採用 Jiagubao 商用加殼軟體進行打包，並採用多種技術確保其可常駐在受感染設備上和躲過安全軟體檢測。

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：

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。

2023/07/31

Remcos遠端存取木馬程式增胖自己來躲避安全軟體偵測

賽門鐵克在最近監控到的惡意網路活動中，發現 Remcos 遠端存取木馬持續以增胖自己的檔案大小（300MB 到 1.5 GB 之間）的伎倆來躲避安全軟體的檢測。它的作法是在動態載入階段以額外的字元覆蓋到惡意檔案。

在二進位檔案的情境，上述所謂的覆蓋是指可以擴展或修改而不影響檔案結構的其餘部分。利用空字元覆蓋，可以有效地增加檔案大小，進而使得整個檔案變大。

以這種方式填充（向檔案新增額外的空字元）不會改變原始檔案的內容或功能，它只會增加整個檔案的大小。進行填充的原因有多種，例如：將資料與特定記憶體邊界對齊或確保區塊大小一致以實現更佳效能的讀寫操作。但在這種情況下，歹徒正在利用它來逃避檢測。雖然檔案非常大，不過一旦經過壓縮，它就會看起來不到 1MB。

歹徒可能會基於各種原因向惡意檔案的覆蓋部分添加空字元，以擴大其檔案大小。這些策略包括安全軟體的檢測會避開特別大的檔案安全檢查、混淆自動分析和沙箱環境、欺騙檔案完整性檢查程序、隱藏額外的有效籌載、以看似合法性來誤導用戶以及規避基於檔案大小的檢測規則。

據觀察，這些膨脹的 Remcos 是透過惡意垃圾郵件、惡意購買關鍵字廣告 (SEO poisoning～搜索引擎最佳化中毒) 和其他網路釣魚網址 (URL) 傳遞。

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：

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訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Trojan/Remcos

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Remcos
- Trojan Horse
- 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：

- System Infected: Trojan.Backdoor Activity 757

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)。