保安資訊--本周(台灣時間2024/04/12)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 48 萬 6,000 台受保護端點上總共阻止了 5,520 萬次攻擊。這些攻擊中有 84% 在感染階段前就被有效阻止：**(2024/04/08)**

- 在**10萬4,700**台端點上，阻止了**1,860**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬3,400**台端點上，阻止了**1,130**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬5,900**台**Windows**伺服主機上，阻止了**9,000**萬次攻擊。
- 在**6萬3,800**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬5,300**台端點上，阻止了**92萬1,200**次嘗試掃描在**CMS**漏洞。
- 在**4萬3,300**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**17萬5,600**台端點上，阻止了**420**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**8,900**台端點上，阻止了**140**萬次加密貨幣挖礦攻擊。
- 在**9萬8,200**台端點上，阻止了**750**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**464**台端點上，阻止了**7萬9,600**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 13 萬 8,100 個受保護端點上阻止了總計 540 萬次攻擊。**(2024/04/08)**

- 使用網頁信譽情資，在 **124.6K** 個端點上阻止 **470** 萬次攻擊。
- 攔截 **28.8K** 個端點上 **537.2K** 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 **11.1K** 個端點上攔截 **130.4K** 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 **413** 個端點上攔截 **19.5K** 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。

2024/04/11

Pupy遠端存取木馬(RAT)持續受到駭客圈青睞，近期針對Linux系統的攻擊，更是明顯

Pupy 遠端存取木馬 (RAT) 一直以來都是駭客組織及個體戶常用的攻擊武器。該惡意軟體具有各種功能，包括檔案的上傳／下載、遠端命令執行、資訊竊取、鍵盤側錄和螢幕截圖偷竊等。儘管 Pupy RAT 已知會針對 Windows 和 Linux 系統，但最近報導的攻擊行動顯示該惡意軟體的 Linux 版本被用於針對亞洲目標的攻擊。

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：

- Packed.Vmpbad!gen38
- 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.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。

2024/04/11

在針對易受攻擊的Redis伺服器攻擊中觀察到Metasploit的高階酬載：Meterpreter

Meterpreter 是 Metasploit 攻擊框架裡的高階酬載，常扮演攻擊鏈後段的滲透測試中，負責建立攻擊方與受害方網路連線的 Stager，它是透過記憶體的 DLL 注入。這個工具已經在駭客圈被列為首選工具有很長一段時間。在最近報導的一次攻擊行動中，發現 Meterpreter 被部署到易受攻擊或配置不當的 Redis 伺服器上。攻擊者還使用一個名為 PrintSpoofer 的提權工具。將Meterpreter 部署到易受攻擊的伺服器是攻擊鏈的初始階段，後續會導致進一步部署任意的酬載，例如：加密貨幣挖礦劫持程式或勒索軟體。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Meterpreter
- Packed.Generic.347
- 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!100
- 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。

2024/04/10

Nitrogen(*氮氣)惡意軟體傳播行動

一場新發動的網路攻擊行動正在傳播 Nitrogen 惡意軟體。該行動濫用 Google 廣告的惡意廣告手法，惡意軟體的二進位檔案偽裝成 PuTTY 或 FileZilla 軟體安裝程式。Nitrogen 使用 DLL 側載入來感染目標系統。一旦部署，這種惡意軟體通常用於獲取初始存取權限，進而推送攻擊鏈達到網路入侵和額外任意有效酬載的佈署。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.NPE
- 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

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。

2024/04/09
防護亮點：賽門鐵克端點偵測與回應(EDR)具有最完整的「防禦規避」偵測能力

「防禦規避」

網路安全被比喻為一場無休止的「打地鼠：whack-a-mole」遊戲。每擊倒一個惡意軟體，似乎就會有另外兩個惡意軟體冒出來。威脅方不斷演變、根據特殊需要加以調整，並開發出更加複雜的攻擊策略。「防禦規避」是任何攻擊鏈中的關鍵因素之一。為了避免被發現並在已入侵的系統中保持常駐能力，攻擊者（通常稱為「對手」）在攻擊鏈／過程中會使用各種技術，例如：停用安全產品、濫用和利用被信任的執行緒、偽裝以及許多其他策略。

根據 MITRE ATT&CK 指南，「防禦規避」是指「攻擊方試圖避免被偵測到」。簡潔有力的定義。然而，「防禦規避」並不簡單，它由數十種技術組成，每種技術都描述攻擊者在試圖入侵目標系統或網路時，為避免被偵測而可能使用的特定方法或伎倆 (作為參考：MITRE ATT&CK 技術是 MITRE ATT&CK 框架的一部分，該框架對攻擊者在網路攻擊的不同階段所使用的方法和戰術進行分類。有數百種不同的攻擊方式，被歸類稱為「戰術」的幾個少數類別中，「防禦規避」就是其中之一)。

賽門鐵克的端點偵測與回應 (EDR：Endpoint Detection & Response)

為了應對這些持續的攻擊，賽門鐵克不斷為其 EDR 產品組合增加新功能，投資於進階防護技術。這些新工具是我們的旗艦產品 Symantec Endpoint Security Complete(SESC) 的特色功能，主要在針對安全問題與 MITRE 攻擊鏈週期的早期攻擊做處理，以快速偵測漏洞並停止正在進行的攻擊。然後，EDR 能夠透過在回應攻擊過程中生成的 EDR 事件來自動繪製並顯示攻擊鏈。

最常用的 MITRE 防禦規避技術包括以下幾種：

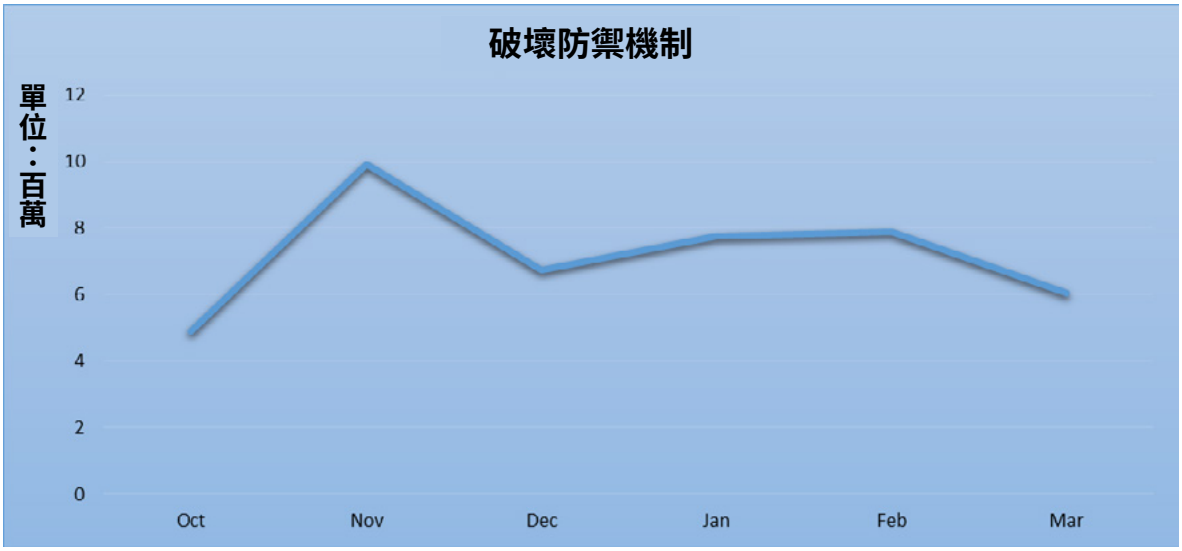
破壞防禦機制 [MITRE : T1562]

這是攻擊方用來停用安全產品的常用手段之一，方法是強制終止處理程序或透過修改登錄機碼來卸載／停用安全產品。

常用方法

- 使用 taskkill 指令來強制終止處理程序
- 使用 netsh 停用防火牆
  - netsh firewall set opmode disable
  - netsh advfirewall set currentprofile state off
- 透過修改相關登錄機碼停用安全軟體

賽門鐵克 EDR 針對攻擊方損害防禦嘗試的可見性



攻擊指標清除 [MITRE : T1070]

入侵者利用這種手法，透過刪除或修改系統內生成的數位軌跡（例如：刪除任意登錄機碼／值、清除瀏覽器歷史記錄、修改日誌等）來妨礙防禦機制。

常用方法的前幾名

- 使用 wevtutil.exe 清除 Windows 事件日誌
  - wevtutil cl security
  - wevtutil cl system
  - wevtutil cl application
- 使用 vssadmin.exe 刪除陰影副本
  - vssadmin delete shadows /All /Quiet

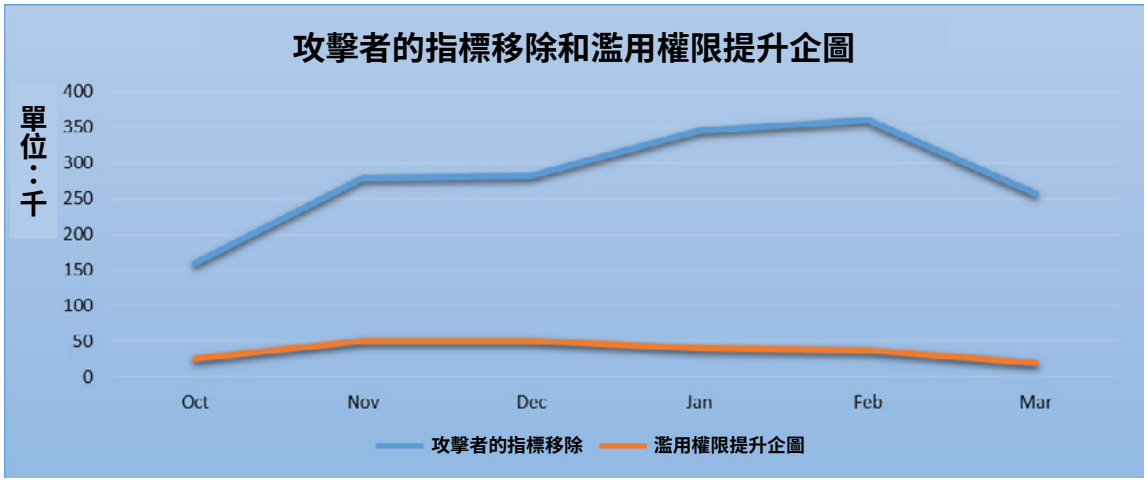
濫用提升控制權限的機制 [MITRE : T1548]

攻擊者透過濫用許可權配置、繞過 UAC、sudo 緩存等技術，來獲得更高的權限。

常用方法的前幾名

- 使用 mmc.exe、fodhelper.exe 繞過 UAC

賽門鐵克 EDR 針對攻擊者的指標移除和濫用權限提升企圖的可見性



從現實世界的角度來看，**勒索軟體**可以說是有史以來最具破壞性和危害性的網路威脅之一，它有多種變種，與我們上面討論那些變種使用類似的防禦規避技術，其中包括：

- Lockbit
- Enmity
- Snatch
- Noberus
- Blackbyte
- Hive

透過直觀簡易的管理與佈署單一平臺／單一代理程式所提供最完整多層次端點防護功能，Symantec Endpoint Security Complete 可解決這些 MITRE ATT&CK 技術和更多問題。從預防到偵測，再到在這場無休止的『打地鼠』遊戲中增強您自己的安全資源，賽門鐵克無時無刻都在創新，日以繼夜捍衛您的資訊安全。

欲深入瞭解有關 Symantec 端點檢測和響應的訊息，請點擊此處。
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。

2024/04/09

假冒AI服務為幌子的臉書廣告，Nova惡意竊密程式從多如牛毛的惡意程式中脫穎而出

據報導，在真實網路情境發現一起新的惡意竊密程式散播行動，攻擊者利用遭入侵的 Facebook 帳戶來宣傳冒充知名品牌，例如：MidJourney、SORA AI、Evoto、ChatGPT-5 和 DALL-E 3 的虛假人工智慧 (AI) 服務。這些廣告引誘受害者下載偽裝成上述人工智慧程式的桌面版本的惡意軟體。Nova Stealer、Rilide Stealer V4、Vidar 和 IceRAT 是在這次行動中散播的惡意竊密程式酬載，已知它們針對來自各個歐洲國家的用戶。

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：

- CL.Downloader!gen211
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2024/04/08

遭駭客入侵接管的YouTube帳戶，散播Vidar和LummaC2惡意竊密程式

威脅行為者不斷改進他們的戰術，以使其惡意軟體散播更加有效。在 YouTube 的內容或評論中隱藏惡意竊密程式似乎不再是一種令人信服的詭計。最近報告顯示，攻擊者轉而致力於駭入並接管知名的 YouTube 頻道，並利用內容創作者的聲譽來誘使訂閱者和隨機的 YouTube 使用者下載惡意軟體。在這種特殊情況下，惡意軟體包括 Vidar 和 LummaC2 惡意竊密程式，它們都以竊取瀏覽器資料以及下載和安裝其他惡意軟體而聞名。

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：

- Scr.Malcode!gdn21
- Scr.Malcode!gdn32
- 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!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。

2024/04/08

Agent Tesla多功能木馬程式，瞄準西班牙公司並利用加密通訊平臺Telegram分享外洩資料

賽門鐵克最近在西班牙發現一個惡意垃圾郵件發送者 (電子郵件主題：FACTURA MES DE MARZO 2024)，聲稱自己是一家西班牙公司，專門為企業提供各種會計、稅務、勞務和審計服務。收件人受到發票／出貨明細騙局的誘惑。如果有人被誘騙打開附件中的 .GZ 壓縮檔 (Facturas Marzo.gz)，然後運行其中的惡意二進位檔案 (Facturas Marzo.exe)，就會被 Agent Tesla 入侵。以下是惡意竊密程式的部分功能：

- 記錄鍵盤輸入
- 竊取網路瀏覽器的登錄憑證
- 竊取電子郵件伺服器的登錄憑證
- 竊取 VPN 密碼
- 竊取 FTP 伺服器的登錄憑證
- 竊取 WinSCP 的登錄憑證

惡意軟體被設置為與攻擊者控制的 Telegram 機器人通訊。在收集竊取的資料並準備傳輸後，惡意竊密程式會利用 Telegram Bot API 將這些資訊以訊息的形式發送到攻擊者的 Telegram 帳戶或群組。惡意竊密程式和遠端存取木馬開發者日益採用這種伎倆。

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：

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：

- Infostealer
- 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: Untrusted Telegram API Connection

基於機器學習的防禦技術：

- Heur.AdvML.B!100

2024/04/08

進階持續威脅(APT)駭客集團：Midge，鎖定俄羅斯和白俄羅斯機構組織

據觀察，進階持續威脅 (APT) 駭客集團：Midge，鎖定俄羅斯和白俄羅斯機構組織。該駭客集團透過傳遞附件為 HTA 檔案的垃圾郵件為初始攻擊。一旦 HTA 檔案被開啟，它就會開始下載並執行遠端 VBA 腳本。然後，腳本會嘗試與其 C&C 伺服器通訊。一旦被感染，攻擊者就會以憑證、網路架構和敏感性資料外洩為目標。

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：

- Trojan.Gen.MBT

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。

2024/04/08

越南駭客組織：CoralRaider濫用.LNK捷徑檔所發動的惡意軟體散播行動正在鎖定亞洲的機構組織

據觀察，由駭客組織：CoralRaider 所發動的惡意軟體散播行動正在鎖定亞洲的機構組織。該駭客組織利用 .LNK 的捷徑檔來誘使受害者下載 HTML 應用程式檔案。涉入的惡意程式是 QuasarRAT 的後繼新變種 Rotbot，能夠用來進行各種檢查並下載最終有效酬載 XClient 惡意竊密程式。XClient 惡意竊密程式能夠收集敏感性資料，包括瀏覽器資料、應用程式資料、社交媒體帳戶、訊息應用程式內容和螢幕截圖。收集到的資料隨後會外洩到其命令與控制 (C&C) Telegram 機器人。

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.Mshta-Http!g1
- ACM.Ps-Http!g1
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen111
- Downloader
- ISB.Downloader!gen63
- Scr.Malcode!gdn32
- Scr.Malcode!gen
- Trojan Horse
- 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
- 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 568
- 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。

2024/04/08

SafeRAT遠端存取木馬

SafeRAT 是最近發現的另一種活躍在威脅領域的遠端存取木馬。該惡意軟體具有剪貼簿竊密程式和鍵盤側錄的功能，可從各種瀏覽器和通訊應用程式中竊取資料，收集受感染機器的資訊，並運行從遠端 C&C 伺服器獲取的其他任意外掛程式。根據最近的報告，SafeRAT 被認為是透過包含惡意 .bat 附件的垃圾郵件傳播的。

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

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.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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: Trojan.SafeRAT Activity
- System Infected: Trojan.SafeRAT Activity 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。

2024/04/08

Magento漏洞CVE-2024-20720

有報告顯示，威脅行為者能夠利用 Adobe Magento Open Source 命令注入漏洞 (CVE-2024-20720)(現稱為 Adobe Commerce) 向某些電子商務網站注入後門惡意軟體。該漏洞允許攻擊者在目標伺服器上執行任意程式碼，可能導致遠端程式碼執行。。

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。

2024/04/07

Vedalia(*維達利亞)進階持續威脅(APT)駭客組織利用超大的捷徑檔(.LNK)發動惡意軟體攻擊行動

據觀察，Vedalia（又稱 Konni）進階持續威脅 (APT) 駭客組織的惡意軟體攻擊行動使用超大的捷徑檔 (.LNK)。威脅行為者利用雙重副檔名來隱藏原始的 .lnk 副檔名，觀察到 LNK 檔包含過多的空白來掩蓋惡意命令列。作為攻擊鏈的一部分，命令列腳本搜索 PowerShell 以繞過檢測並定位嵌入檔和惡意有效酬載。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen20
- Scr.Mallnk!gen13
- Trojan.Gen.NPE
- WS.Malware.1

2024/04/07

Seedworm駭客集團如火如荼散播遠端系統管理軟體代理

在魚叉式網路釣魚行動中發現一個針對歐洲、中東和非洲地區的駭客集團--Seedworm(又稱MuddyWater)。攻擊者透過上架在雲端空間伺服器上的 PDF 檔案附件，傳遞 Atera 和 ConnectWise ScreenConnect 遠端系統管理軟體的代理程式。這些代理程式一經執行，就會授予威脅者遠端存取遭入侵系統的權限，允許他們執行檔案的操作。

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)：

- PUA.Gen.2

- Trojan.Malmsi
- 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：

- Audit: Atera Client Activity
- Audit: TLS v1 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。

2024/04/07

SecTopRAT惡意木馬，假冒NordVPN安裝程式大肆傳播

最近發現一起利用微軟的必應 (Bing) 廣告，來推廣虛假 NordVPN 安裝程式的惡意廣告行動，最終會植入 SecTopRAT，這是一個基於 .NET 的木馬程式，可以從受害者的電腦中竊取敏感個人資訊。

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：

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!500
- 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。