保安資訊--本周(台灣時間2024/03/29)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 52 萬 8,800 台受保護端點上總共阻止了 5,860 萬次攻擊。這些攻擊中有 81.2% 在感染階段前就被有效阻止：**(2024/03/26)**

- 在**10萬7,800**台端點上，阻止了**1,880**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**13萬9,700**台端點上，阻止了**1,200**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**3萬7,500**台**Windows**伺服主機上，阻止了**9,200**萬次攻擊。
- 在**6萬6,500**台端點上，阻止了**200**萬次嘗試掃描伺服器漏洞。
- 在**1萬4,500**台端點上，阻止了**85萬5,400**次嘗試掃描在**CMS**漏洞。
- 在**4萬5,900**台端點上，阻止了**140**萬次嘗試利用的應用程式漏洞。
- 在**19萬4,100**台端點上，阻止了**480**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1萬9,500**台端點上，阻止了**350**萬次加密貨幣挖礦攻擊。
- 在**10萬7,500**台端點上，阻止了**770**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**714**台端點上，阻止了**9萬8,600**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 14 萬 7,000 個受保護端點上阻止了總計 590 萬次攻擊。**(2024/03/19)**

- 使用網頁信譽情資，在 **132.6K** 個端點上阻止 **520** 萬次攻擊。
- 攔截 **30.5K** 個端點上 **546.1K** 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 **12.3K** 個端點上攔截 **139.8K** 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 **418** 個端點上攔截 **25.6K** 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。

2024/03/28
CVE-2024-20767--Adobe ColdFusion漏洞

CVE-2024-20767 是 Adobe ColdFusion 的一個目錄遍歷漏洞，Adobe ColdFusion 是一個用於建立和部署網頁及行動手機 APP 的開發平臺。例如：成功開採濫用該漏洞，未經認證的遠端攻擊者可在系統上讀取任意檔案。賽門鐵克的網路防護技術入侵防禦系統 (IPS) 可阻擋這些漏洞的攻擊嘗試，防止系統受到進一步感染或損害。

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: Passwd File Download Attempt
- Web Attack: Adobe ColdFusion Arbitrary File Read CVE-2024-20767

2024/03/28
Sync-Scheduler(*同步調度)惡意竊密程式

一種名為 Sync-Scheduler 的惡意竊密程式，採用 C++ 撰寫，據報導被隱藏在 Office 文件檔中進行傳播。該惡意軟體採用檔案巢狀結構 (file-nesting) 技術來隱藏自身，並配備反分析和防禦規避技術。在入侵系統後，它會搜索使用者個人目錄中的 Office 文件檔，例如：Word、PowerPoint 和 Excel 文件。然後，竊取的資料會以表單數據形式透過網路外洩。

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.MalTraffic!gen1

檔案型(基於回應式樣本的病毒定義檔)防護：

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

基於機器學習的防禦技術：

- Heur.AdvML.A
- 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 Process Request 4
- 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。

2024/03/28

WarzoneRAT惡意軟體以全新變種捲土重來

WarzoneRAT (也被稱為 AveMaria) 是一種商品化的遠端存取特洛伊木馬，近年來被各種威脅組織使用。惡意軟體功能包括遠端控制、遠端 Shell 和檔案操作、憑證竊取、鍵盤側錄、使用者帳戶控制 (UAC) 繞過等。就在 2024 年 2 月，FBI 摧毀 Warzone RAT 惡意軟體的運作，並查獲與該威脅相關聯的基礎設施。就在最近，發現新的 WarzoneRAT 惡意軟體樣本在真實網路情境又出現，表明這種威脅有可能捲土重來。多階段攻擊鏈涉及惡意垃圾郵件、LNK 捷徑檔和 HTA 網頁格式檔去呼叫與執行 VBScripts 和 PowerShell 命令，最終引爆 Warzone 有效酬載的結果。

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-Cmd!g1
- ACM.Mshta-Ps!g1
- ACM.Ps-Http!g2
- ACM.Ps-Mshta!g1
- ACM.Ps-Wscr!g1
- ACM.Rgsvc-Lnch!g1
- ACM.Wscr-Ps!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen241
- Infostealer
- Scr.Mallnk!gen13
- Scr.Malscript!gen11
- 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.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- 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 795
- 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。

2024/03/28

TheMoon惡意軟體瞄準數千個不安全的路由器

據報導，一場全新的惡意攻擊行動，涉入的是 TheMoon 惡意軟體的後繼新版本，這是一個惡名昭彰的惡意軟體家族。這個最新 TheMoon 後繼新變種似乎瞄準不安全的老舊家用路由器，特別是由「華碩」製造的路由器，以及其他物聯網設備。這些設備遭感染後，惡意軟體利用它們透過一個名為 Faceless 的代理服務來路由流量。它積極尋找特定 shell 環境來執行其主要的惡意酬載，並與威脅行為者的命令和控制伺服器 (C&C) 建立連接，以接收進一步的指令。

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：

- 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。

2024/03/28

小心 FlightNight(*夜間飛行)攻擊行動

觀察到一個全新的威脅行為者採用類似於近期才針對印度政府實體 Go-Stealer 攻擊行動的戰術、技術和程序 (TTPs)。FlightNight 因其使用名為『FlightNight』的 Slack 頻道而得名，很可能是同一威脅行為者的作品。利用修改版的開源工具 HackBrowserData，它針對印度政府實體，包括負責電子通訊、IT 治理和國防的部門。

偽裝成來自印度空軍的邀請函的釣魚郵件包括一個 ISO 檔附件。隨附的 PDF 檔誘騙受害者執行快速操作流程的捷徑，然後安裝惡意軟體。FlightNight 隨後可以竊取 Microsoft Office 文件檔、PDF 檔案、SQL 資料庫和網頁瀏覽器的歷史記錄、Cookie、快取等機密資訊。

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：

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 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!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。

2024/03/27

偽裝成合法PuTTy軟體的惡意程式植入器

據報導，一名威脅行為者購買一則自稱是 PuTTY 主頁的廣告。這則廣告出現在 Google 搜索結果頁面的頂部，儘管後來已被移除。它出現在官方 PuTTY 網站之前。這則廣告引起懷疑，因為其網域名稱與 PuTTY 無關。廣告中宣傳的 PuTTY 檔實際上是惡意軟體，是用 Go 語言撰寫的惡意程式植入器。執行後，該惡意程式植入器將傳遞最終的有效酬載，即所謂的 Rhadamanthys 惡意竊密程式。

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
- 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。

2024/03/27

Mispadu惡意竊密程式正在開疆闢土

Mispadu 惡意竊密程式 (也稱為 Ursa) 在最近的惡意軟體散播行動中，顯示出一些增加的活動。雖然這種惡意軟體最初主要針對拉丁美洲國家，但最近觀察到的活動也顯示出對歐洲國家為目標。該惡意軟體感染鏈利用內嵌惡意網址的 pdf 文件檔，可以下載包含惡意的 MSI 安裝程式或 HTA 腳本的 .zip 壓縮檔。後續階段包括部署惡意的 VB 腳本和 Mispadu 惡意軟體酬載。

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-Mshta!g1
- ACM.Ps-Wscr!g1

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.3

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。

2024/03/27

Qilin(*麒麟)勒索軟體仍然是網路安全中的活躍威脅

Qilin 又稱 Agenda，是一種採用 Rust 語言撰寫的勒索軟體，於 2022 年被發現。這種惡意軟體最近幾個月在真實網路情境大肆傳播，新版本中不斷出現新的發展。Qilin 以勒索軟體即服務(RaaS) 模式進行傳播，其運營商經常採用雙重勒索戰術。最近攻擊行動中，大多數使用自訂 PowerShell 腳本來攻擊 vCenter 和 ESXi 實例。

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.Untrst-RLsass!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Cryptlocker!g42
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253
- SONAR.TCP!gen1
- SONAR.TCP!gen6

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Agenda
- Ransom.Qilin
- Ransom.Qilin!g1
- Trojan.Gen.MBT
- Trojan Horse
- Web.Reputation.1
- 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

2024/03/27

SnowLight惡意程式下載器在開採濫用F5 BIG-IP和ScreenConnect漏洞的攻擊行動中傳播

最近據報告，歸因於 UNC5174 威脅組的惡意行動採濫用 F5 BIG-IP(CVE-2023-46747)和 Connectwise ScreenConnect(CVE-2024-1709) 漏洞進行惡意軟體傳播。其中一種惡意軟體 SnowLight 是採用 C 語言撰寫的 Linux 平台之惡意程式下載器，被威脅行為者用來在感染的機器上下載並執行後續有效酬載。GoreVerse、GoHeavy 和 SuperShell 是 UNC5174 在報告行動中分發的不同酬載。

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：

定義檔)防護：

- Backdoor.Trojan
- Trojan Horse

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: F5 BIG-IP RCE CVE-2023-46747
- Web Attack: ConnectWise ScreenConnect CVE-2024-1708
- Web Attack: ConnectWise ScreenConnect CVE-2024-1709

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，針對 Windows 伺服器的 DCS 預設強化政策可防止任意命令和 powershell 的執行，並防止篡改重要 Windows 作業系統檔和資料夾。
- 可對政策中的 DCS 網路規則進行配置，以將 ScreenConnect 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。

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。

2024/03/26
防護亮點：「調適型防護：Adaptive Protection」如何幫助資安團隊阻止不斷變化的威脅

身為首席資安長 (CISO) 或安全營運中心 (SOC) 的成員，威脅形勢不斷帶來新的挑戰，其中「勒索軟體攻擊」和「就地取材」的戰術尤其普遍且更具破壞性。這些威脅通常會利用企業內部的合法工具和流程，使其難以在不中斷基本業務運作的情況下被發現和緩解。

賽門鐵克的「調適型防護」功能為此難題提供重要的解決方案。它讓客戶監控並阻止企業內發生的一般應用程式行為，同時透過自動白名單允許合法的使用案例。它使企業能夠主動防禦勒索軟體和其他惡意活動，同時最大限度地減少對日常營運的干擾。

分析最近的安全事件可以發現一個令人擔憂的趨勢，即 AlphaV、Lockbit 和 Play Ransomware 等駭客組織利用各種通用的應用程式之行為來實施惡意活動。利用 Screenconnect、PsExec 和 VssAdmin 等工具進行未經授權的系統存取、網路內橫向移動和系統操控。同樣的，他們也利用 7Zip 隱藏惡意有效酬載，利用 AnyDesk 進行未經授權的系統存取，進而實現資料滲出和惡意軟體部署。此外，攻擊者還利用 PowerShell、PsExec 和 WinRAR 來執行指令、部署惡意軟體、提權、混淆有效酬載或資料洩漏。

為了說明客戶如何使用我們的「調適型防護」功能，請參考 2023 年 9 月這份範例。某客戶已經將 126 種行為設置為拒絕，並希望進一步加強其安全態勢。他們採取的步驟如下：

1. 利用 Adaptive Protection 的熱圖，可深入評估環境中的軟體或工具的行為洞察力。
2. 確定了一組處於監控模式且未在公司使用的行為。具體方法是識別熱圖頁面上的深藍色（零發生率）項目。
3. 使用威脅分類按鈕過濾來識別任何非深藍色但被視為「拒絕」的風險行為。
4. 檢查系統生成的例外情況，將正常業務操作行為列入白名單。
5. 更新「調適型防護」政策，在「拒絕」模式中新增新行為。

雖然並非所有基於「調適型防護」的特徵都被切換為拒絕，但該客戶選擇為他們提供額外的保護，以抵禦一次 Lockbit 著名勒索軟體組織的攻擊。以下是賽門鐵克截至 2024 年 1 月 19 日「調適型防護」軟體監控到「就地取材-Living off the Land」攻擊的細項：

- 未受信任的程序修改登錄檔上的自動執行的機碼註 (autorun)
- 未受信任的程序修改工作排程
- 透過 Netsh 停用安全性設定
- 轉存作業系統憑證
- 使用 Netscan 收集環境資訊
- 使用 Psexec 執行程式碼
- 使用 rclone 將資料移出網路
- 以 Powershell 建立可執行檔
- 使用 Bcdedit 停用還原
- 以 Powershell 呼叫 VSSAdmin 刪除備份

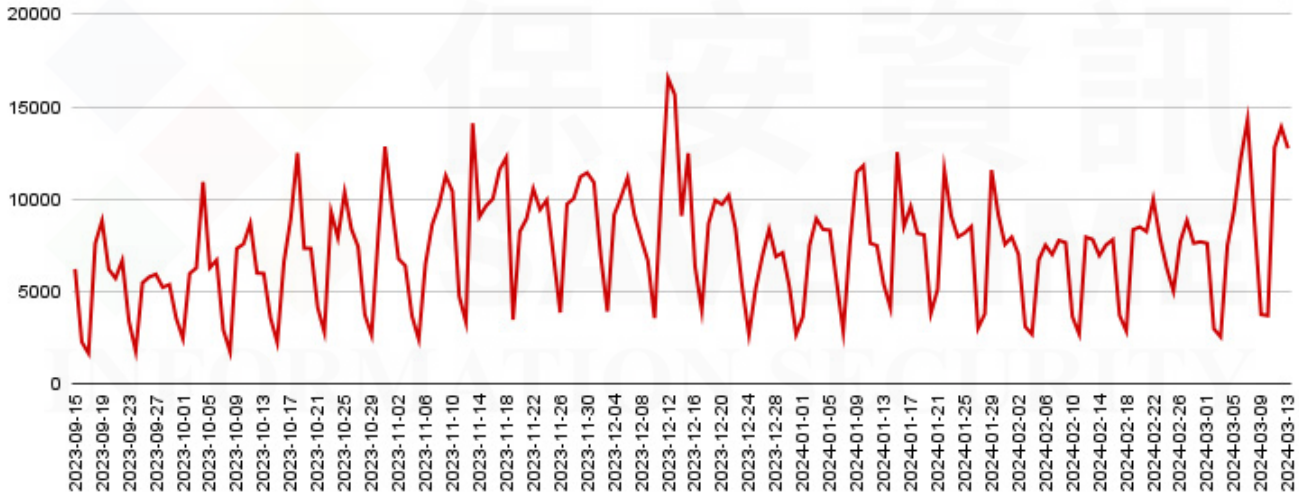
- 以 Powershell 呼叫 WBadmin 刪除備份
- 以 Fsutil 刪除勒索軟體可執行檔的痕跡
- 以 Powershell 下載有效酬載

此類攻擊利用許多系統工具來執行各種任務，從程式碼執行到清除惡意軟體存在的痕跡。有人看到這個清單後可能會認為，他們可以在自己的環境中為所有這些行為開啟拒絕功能--這很好！但是，每個客戶的需求都不盡相同，而「調適型防護」可以量琛打造更靈活地確保最大程度的安全性，同時將干擾降到最低。

總之，「調適型防護」在客戶中的使用證明它的有效性和廣泛應用。

- 469 種行為可設置為拒絕模式。
- 平均每個客戶有 338 種行為被設置為拒絕模式。
- 目前有 150 多萬台機器受到該功能的保護。
- 因此，每天大約有 8,000 個行為被阻止。

「調適型防護」每天攔截的「就地取材」攻擊數量



雖然被攔截的行為數量看似不多，但關鍵是要認識到這些行為與標準或正常的工具有關而非惡意軟體。傳統的安全技術可能無法發現這些活動，但如果不加以妥善管理，它們有可能造成重大損失。這凸顯了「調適型防護」在識別和緩解濫用日常工具的威脅方面的重要性，進而確保環境更加安全。

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「調適型防護」功能的更多資訊，請點擊此處。

2024/03/26

Stately Taurus駭客組織針對亞洲國家的網路攻擊行動

研究人員在本月剛剛舉行「東協與澳洲2024年特別峰會」期間，觀察到最近一次針對亞洲國家由中國駭客組織 Stately Taurus (又名 Mustang Panda) 所發動的網路攻擊行動。在最近的這次攻擊中建立並部署兩個惡意套裝軟體，一個是 ZIP 格式的壓縮檔，另一個是 .SCR 的螢幕保護檔。這兩個套裝軟體主要目的都是利用假冒 QFX Sofware 公司和 Electronic Arts 公司等知名軟體開發商的應用程式來部署惡意軟體。

初始感染是從一個可執行檔開始的，隨後會側載一個惡意 DLL，最後一步是載入一個解密後的編碼，以便在受害者的機器與攻擊者的專用 C&C 伺服器之間建立連線，以便能夠進行網路間諜活動。

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：

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

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。

2024/03/26

VCURMS和STRAT遠端存取木馬(RAT)透過垃圾郵件中的連結發送

發現一個 Java 下載器可傳播 VCURMS 和 STRRAT 遠端存取木馬 (RAT)。該下載程式透過電子郵件與惡意 JAR 檔的連結進行部署。然後，這兩個 RAT 會下載經過修改的 Rude 惡意竊密程式和鍵盤記錄程式，進行資料外洩。

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.Maljava

- Trojan.Gen.NPE
- Trojan Horse

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。

2024/03/25

全新後門程式：WineLoader

發現假冒政黨名義的網路釣魚攻擊來部署 WineLoader 惡意軟體，並邀請外交官參加品酒會。WineLoader 是一種全新的惡意後門程式，其特徵與 APT29 駭客組織相關連的 BurntBatter、BeatDrop 和 MuskyBeat 惡意程式相似。一旦被部署，WineLoader 就會從受感染的機器上收集資訊(包含受害者的帳號、程序名稱、設備名稱等）並將其外洩到 C&C。C&C 可決定執行其他模組，以執行建立持續性等進一步任務。

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

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gen
- Trojan.Gen.MBT
- Trojan.Malscript
- WS.Malware.1
- Web.Reputation.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: Suspicious Process Accessing Lets Encrypt Certified Site
- Web Attack: Webpulse Bad Reputation Domain Request

2024/03/25

中國出現利用惡意驅動程式的新型遠端控制後門

最近在中國觀察到的網路攻擊行動中，傳播一種新的遠端控制後門。該行動幕後的威脅者利用惡意內核模式驅動程式 (kernel-mode drivers) 來開啟行動。該後門具有多種功能，包括停用防毒軟體、鍵盤側錄以及從命令與控制 (C&C) 伺服器下載其他的惡意程式 (例如：挖礦和 rootkit) 以供後續執行。該行動突顯出，威脅者將繼續利用 rootkit 隱藏惡意程式碼，使其無法被安全工具發現，進而削弱防禦能力並長時間逃避檢測。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Malfilter
- 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。

2024/03/25

源於Mirai殭屍網路的新變種：Mirai Nomi

在威脅環境中出現一種源於 Mirai 殭屍網路的新變種被稱為：Mirai Nomi。該變種特徵是經 UPX 封裝、用於指揮和控制的時間依賴型的網域生成演算法 (DGA) 以及多種加密和雜湊演算法。它具有檔案刪除、程序終止、常駐和消除競爭機器人等功能。雖然它並不十分活躍，但其能力引起人們對未來潛在威脅的擔憂。

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
- 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。