SONAR同時採用多重先進技術防護「就地取材(LOTL)」程序和兩用工具的威脅

2024 年 5 月 14 日發布

何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？

行為分析這種即時防護，可在電腦上執行應用程式時偵測潛在惡意的行為。行為分析使用啟發式技術及信譽資料來偵測新出現和不明威脅。行為分析提供「零時差」防護，因為它會在傳統病毒和間諜軟體偵測定義檔建立前偵測惡意行為，從而解決威脅。行為分析可為您的用戶端電腦提供額外的防護等級，並能與您現有的病毒和間諜軟體防護、入侵預防、記憶體攻擊緩和以及防火牆防護相輔相成。行為分析使用啟發式系統，該系統會運用賽門鐵克的線上威脅情資網路，並且對用戶端電腦進行主動型本機監視，以偵測新出現的威脅。行為分析也會偵測您應監視之用戶端電腦上的變更或行為。

SONAR

賽門鐵克的行為分析技術被稱為「SONAR」，我們將在本防護公報中使用這個專用術語。SONAR 可透過追蹤跨檔案譜系、登錄檔、程序譜系、服務、執行緒插入、DLL 側載和程序空白技術等複雜攻擊鏈。它還能追蹤攻擊鏈中合法程序的使用情況。其中包括「就地取材 (LOTL)」程序和兩用工具。一旦識別出惡意向量 (方法／途徑／酬載)，SONAR 就會刪除惡意檔案、登錄項目和程序，並終止攻擊中使用任何 LOTL 和兩用工具的程序，進而瓦解整個攻擊鏈。

AutoIt：凸顯「就地取材(LOTL)」程序和兩用工具的資安風險

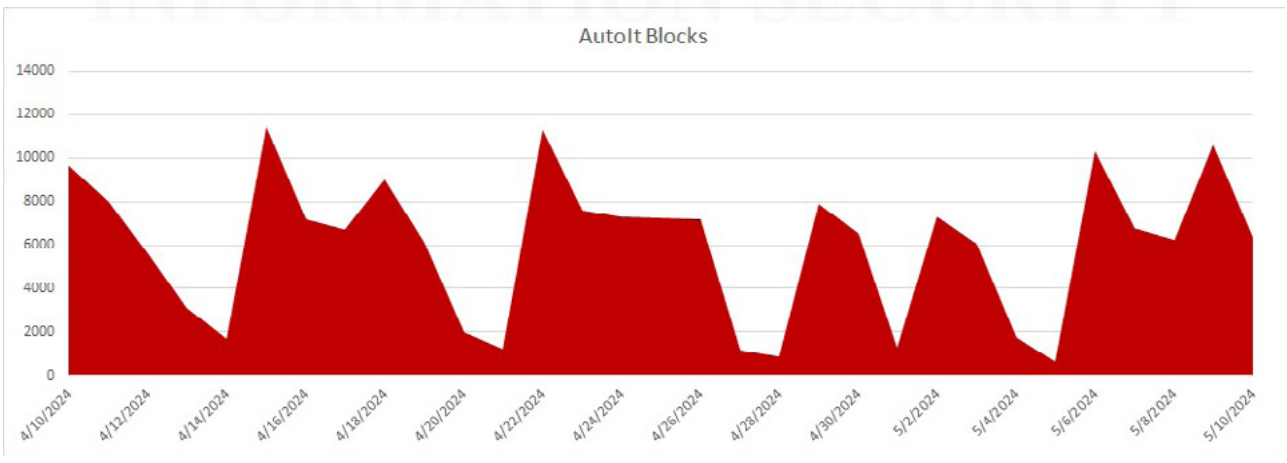
AutoIt 是使用於 Windows 平台的自動腳本語言，可用來建立自動化執行腳本的免費自動化工具。一些惡意軟體家族 (例如：Darkgate 和 Astaroth) 在攻擊鏈中安裝並濫用 AutoIt，從可信任的協力廠商程式中執行惡意腳本。這些基於腳本的有效酬載通常都經過混淆化 (Obfuscation)，以逃避靜態偵測技術的偵測，但無法輕易躲過行為偵測技術的檢測。

SONAR 採用多重技術防護「就地取材 (LOTL)」程序和兩用工具的威脅：

1. 我們追蹤程序的起源，例如二進位檔案是如何被導入以及程序是如何啟動的。它可觸發對可疑程序起源的行為檢測，例如：AutoIt 由不尋常的父系程序啟動 (例如：SONAR.SuspBeh!gen804)，或 AutoIt 被掏空 (例如：SONAR.SuspStart!gen18)。
2. 我們監控攻擊鏈中所有程序的所有行為。AutoIt 可被運用於多種惡意情境，包括下載額外的有效酬載 (例如：SONAR.Dropper!gen2) 和啟動程序，以進一步實施攻擊 (例如：SONAR.SuspLaunch!g220)。
3. 我們確保終止所有涉入攻擊的 LOTL 和兩用程序。遭濫用的 AutoIt 程序往往就是攻擊鏈中的關鍵。若僅刪除其他被檢測到的程序／元件而不刪除 AutoIt 程序，會使系統受到進一步攻擊和再次感染。

無論我們是直接從行為偵測技術檢測到遭濫用的 AutoIt 程序，還是檢測到攻擊的其他元件 (例如：賽門鐵克靜態資料掃描檢測到的惡意檔注入，或賽門鐵克網路層入侵防禦技術 IPS 檢測到 C&C 流量)，SONAR 都會追蹤遭濫用的 AutoIt 實例，可以避免攻擊鏈初始階段的星星之火，延燒成重大資安事件的燎原大災難。(例如：AGR.Terminate!g2)。

SONAR 每天攔截數千次源於 AutoIt 遭濫用的攻擊



SONAR 有效防護 AutoIt 遭濫用的實例，只是我們全球資安專家團隊日以繼夜分析的無數威脅向量 (方法／途徑／酬載) 和惡意軟體家族中的其一例子。最新 SONAR 行為保護技術透過每日數次的持續更新。

要了解更多有關 Symantec Endpoint Protection 行為分析技術 SONAR 的資訊，請點擊此處。
要了解有關啟用 SONAR 的更多資訊，請點擊此處。
SONAR 還與 Symantec Cloud Sandbox 整合。要了解 SONAR 和 Symantec Cloud Sandbox 如何協同工作來檢測 Monster Stealer，請點擊此處。

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 年起就全心全力於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環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。保安資訊連絡電話：**0800-381-500**。

2024/05/03

最近傳播Darkgate惡意程式的垃圾郵件行動

該攻擊行動的初始感染鏈是從一個帶有 HTML 附件的電子郵件開始。該 HTML 檔使用的背景圖片看起來像一個空白的 Microsoft 文件，在該檔案中可以看到如何修復離線檢視的檔案說明。這是企圖誘騙受害者將惡意 PowerShell 程式碼貼到 Windows 終端機。程式碼執行後，將下載一個 HTA 檔案並繼續執行，最終下載一個後續的 ZIP 檔。解壓縮後，它會啟動 AutoIt 的開源自動化引擎，執行 script.a3x 的惡意 AutoIt 腳本，最終載入 Darkgate 木馬。

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-Ps!g1
- ACM.Ps-CNPE!g1
- ACM.Ps-CPE!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- AONAR.SuspBeh!gen804

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：

- ISB.Downloader!gen48
- ISB.Heuristic!gen106
- Trojan.Darkgate
- WS.Malware.1
- WS.SecurityRisk.4

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

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。

2024/02/21

Astaroth、Mekotio和Ousaban？三支金融木馬亂奔駭帳號

最近發現有三種銀行木馬在針對拉丁美洲使用者的資訊中利用惡意 run.app 連結。這些連結會將使用者重導向到一個 MSI，該 MSI 會發送 Astaroth(之後會發送 Ousaban) 或 Mekotio。

觀察到惡意垃圾郵件中出現的主旨內容：

- Advertencia AFIP：Datos de registro desactualizados - Riesgo de bloqueo.
- Aviso de Factura：Pendiente de Autorización
- Factura de Servicios：Detalles Adjuntos
- Factura Mensual：Resumen de Cargos

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.SuspPE!gen32

檔案型(基於回應式樣本的病毒定義檔)防護：

- Downloader
- Trojan.Dropper
- Trojan Horse
- WS.Malware.1
- WS.Malware.2

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)。

基於機器學習的防禦技術：

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