駭客想搭便車，門都沒有--賽門鐵克持續領先的SONAR行為防護技術有效偵測和封鎖惡意程序注入與程序挖空

2025 年 1 月 21 日發布

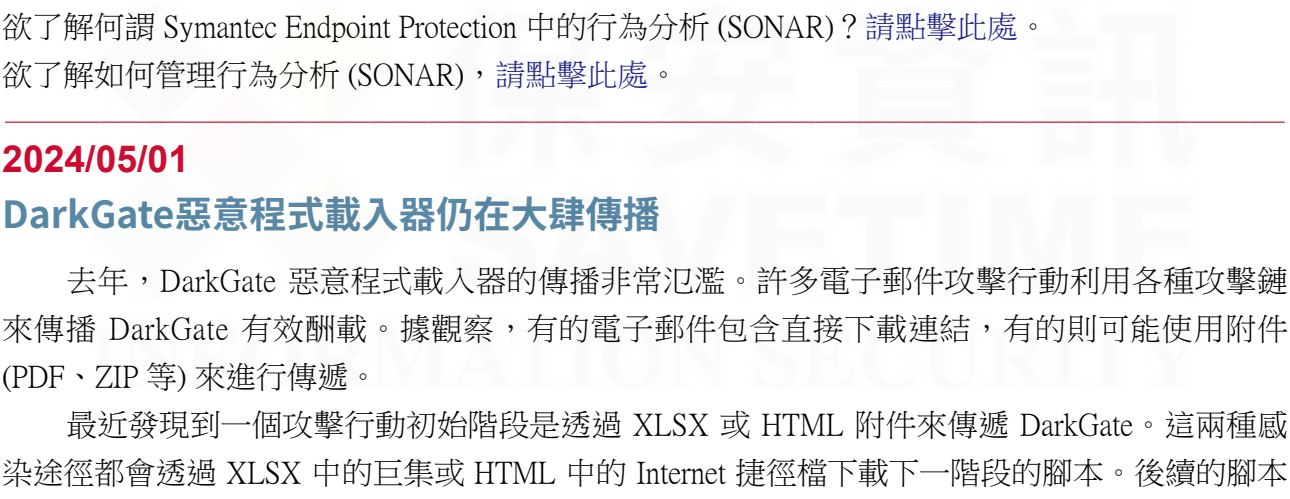
程序注入與程序挖空伎倆

就像最近在 DarkGate 惡意木馬病毒程式攻擊事件中看到，駭客通常會加入一個元件，利用受信任的程序來推進攻擊鏈或傳送有效酬載。程序注入和程序挖空是用來攻擊受信任程序和逃避偵測的兩種伎倆。即使偵測並移除明顯的惡意程序，這些「遭入侵」程序仍可在背景中繼續惡意軟體攻擊。

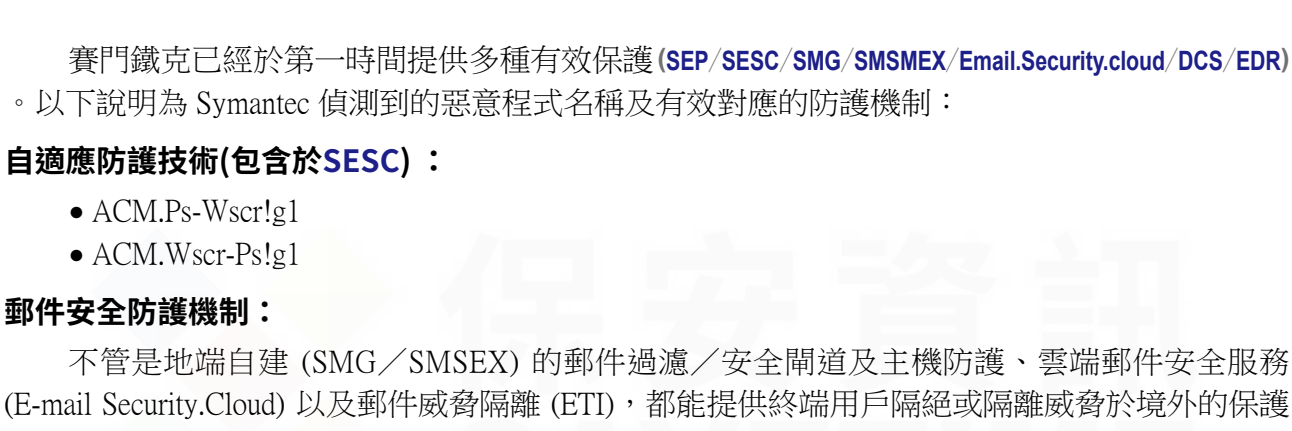
SONAR(Symantec Online Network for Advanced Responce--前瞻回應線上網路) 是賽門鐵克的一種行為偵測的技術，可以在建立病毒定義檔及間諜軟體偵測定義檔前，阻止惡意程式碼侵入。行為防護會持續監控所有程序，無論是否受信任。行為分析這種即時防護可在電腦上執行應用程式時偵測潛在惡意的行為。行為分析使用啟發式技術及信譽資料來偵測新出現和不明威脅。行為分析提供「零時差」防護，因為它會在傳統病毒和間諜軟體偵測定義檔建立前偵測惡意行為，從而解決威脅。我們的安全回應工程師持續專注地研究駭客為了在您的網路立足而使用的最新技術。最新的啟發式技術和防護內容會透過線上自動更新機制 (Live Update) 每週傳送 4 次。

下面圖表顯示 2024 年的資料，證明 SONAR 在偵測和封鎖這些程序注入和程序挖空攻擊方面卓有成效。一旦偵測到「受攻擊」的程序並阻擋惡意行為，SONAR 攻擊群組矯正技術 (Attack Group Remediation--AGR) 就會自動啟動，確保整個攻擊鏈被瓦解。

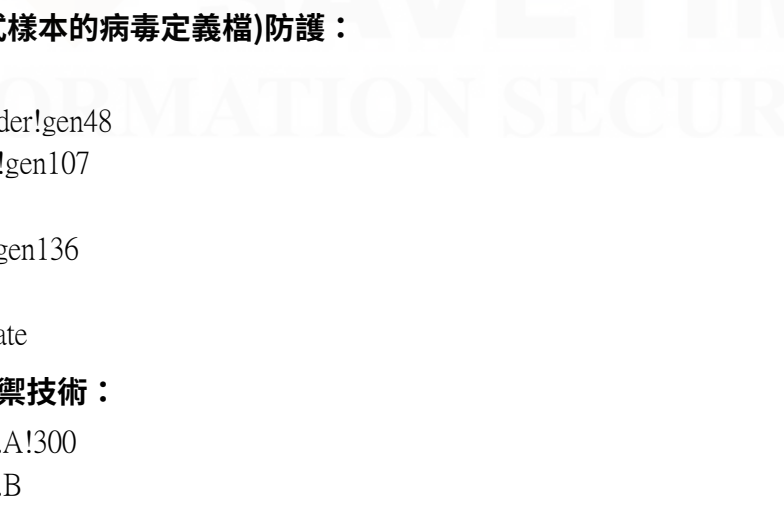
攔截程序注入與挖空的數量



SONAR攻擊群組矯正技術(Attack Group Remediation-AGR)有效解除程序注入或程序挖空的可信任程序



最常遭受程序注入與程序挖空伎倆攻擊的受信任程序



欲了解何謂 Symantec Endpoint Protection 中的行為分析 (SONAR)？請點擊此處。
欲了解如何管理行為分析 (SONAR)，請點擊此處。

2024/05/01

DarkGate惡意程式載入器仍在大肆傳播

去年，DarkGate 惡意程式載入器的傳播非常氾濫。許多電子郵件攻擊行動利用各種攻擊鏈來傳播 DarkGate 有效酬載。據觀察，有的電子郵件包含直接下載連結，有的則可能使用附件 (PDF、ZIP 等) 來進行傳遞。

最近發現到一個攻擊行動初始階段是透過 XLSX 或 HTML 附件來傳遞 DarkGate。這兩種感染途徑都會透過 XLSX 中的巨集或 HTML 中的 Internet 捷徑檔下載下一階段的腳本。後續的腳本執行最終會衍生 DarkGate 惡意軟體有效酬載。

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：

自適應防護技術(包含於SESC)：

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

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
- ISB.Downloader!gen48
- ISB.Heuristic!gen107
- Phish.Html
- Scr.Malcode!gen136
- Trojan Horse
- Trojan.Darkgate

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。

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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。