攻擊群組矯正

2023 年 5 月 22 日發布

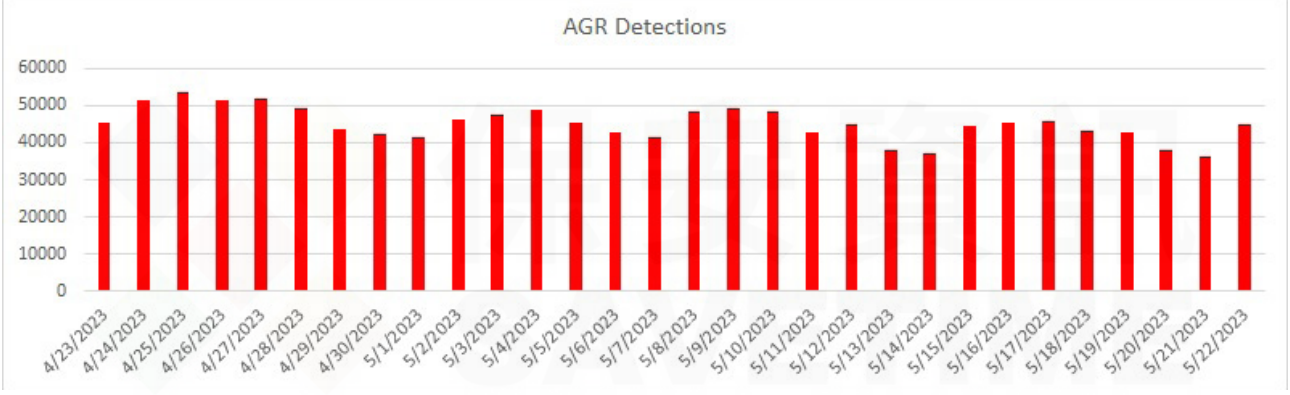
在世界各地，網路攻擊每天的數量都在不斷增加。且越來越複雜、越來越大膽。網路安全供應商無時無刻都不能忽略它們，否則壞人會找到方法進入。不幸的是，他們有時確實會進入。這使得資安業者需要更迫切的發揮創造力，想方設法打擊網路犯罪分子並保護我們客戶最重要的資產與商譽。

雖然靜態偵測定義檔仍然可以發揮作用並且可能永遠都會發揮作用，但行為偵測無疑是時代的潮流。靜態定義檔就像一個電燈開關--要麼開要麼關，即檔案要麼好要麼壞--行為分析技術可以確定壞的程度。與行為分析相結合可以更加確定該行為是否“足夠糟糕”而需要攔截。補充一點，有時合法但寫得不好的程式碼可能表現得很糟糕，但顯然不應該被攔截。

賽門鐵克行為安全技術致力於保護網路免受無檔案式 (Fileless) 攻擊、就地取材 (LOTL)、與基於行為的攻擊。這些動態技術監控端點上的所有相關活動，了解正常的應用程式行為模式，並經過訓練（個別實際情境）以提醒或快速阻止偏離規範的行為。連同行為分析和系統啟發 (BASH) 和行為政策強制執行 (BPE)，攻擊群組矯正 (AGR) 是這些其中的技術。AGR 是最近推出的一項功能，可識別檢測到攻擊中的所有元件，並確保刪除屬於攻擊的每個程序(Process)和執行序 (thread)。

- 傳統的惡意軟體檢測會阻止或矯正惡意軟體。單就這一點通常就足以有效地阻止攻擊。但未必每一次都有效。
- 惡意軟體通常利用包含多個可供發動就地取材攻擊 (LOTL) 的合法程序的複雜攻擊鏈。如果這些程序中的任何一個仍在執行，即使檢測到並刪除關鍵元件後，攻擊也可以重新啟動或繼續。
- AGR 會套用 BASH 群組功能，以透過追蹤程序譜系、檔案譜系和執行緒插入，將程序和檔案放入動態產生的群組中。只要偵測到惡意軟體，會判定整個群組有威脅。
- 若要判定群組有錯，AGR 會尋找群組中的每個執行中程序，並透過特殊 BPE 特徵來判定每個程序有錯。

每天，AGR 都會終止數十萬個惡意程序 (Process) 並破解多種威脅的攻擊鏈，包括後門程序、加載程序、竊密程序、勒索軟體等。僅在過去 30 天內，我們的遙測系統就記錄超過一百萬個攔截的實例。



我們最近發布一份關於 Mallox 勒索軟體的防護公告，它仍然非常活躍地鎖定全球的企業和組織。顯然針對這種威脅採取多種保護措施（第一時間就攔截任何惡意軟體顯然比為了正確命名而忽略它要好），您會注意到 AGR.Terminate!g2 就是其中之一。為了證明這種行為技術的有效性，我們的惡意軟體分析師測試一些最近的 Mallox 勒索軟體樣本，並確認幾乎所有樣本都被 AGR 捕獲（未被 AGR 阻止的內容被其他檢測阻止而大量被記錄）。好結果應該繼續下去。提升創新及改進速度的永無止境的動力必須繼續下去。

查看先前提到攻擊群組矯正 (AGR) 公告列表，請點擊此處。
要了解賽門鐵克行為安全性技術如何防禦就地取材(Living Off the Land)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。

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**。