賽門鐵克進階機器學習(AML)攔截零時差攻擊

2024 年 11 月 26 日發布

賽門鐵克如何利用進階機器學習(AML)技術防禦零時差威脅

機器學習 (Machine Learning)，通常簡稱為 ML，是一種無須特徵檔的技術，可在執行前階段攔截全新的惡意軟體。在博通賽門鐵克 (Broadcom-Symantec) 裡，ML 用於不同層級，以保護我們的客戶免受網路威脅。這些層級的設計可主動或被動「監控」我們產品所看到的可疑檔案、作業系統事件、登錄檔、網頁位址或網路活動的每個位置--包括端點、閘道和我們的後端分析平台。賽門鐵克能夠透過一套完整的威脅掃描引擎，在新內容出現時立即進行動態分析，並將資料擷取至賽門鐵克全球智慧網路 (GIN)。賽門鐵克使用來自數百萬個端點的安全遙測資料、來自第三方安全供應商的威脅相關資料饋送，以及豐富的乾淨檔案集，來訓練和評估各種 ML 模型。這些模型部署在許多產品上，以偵測威脅，包括作為我們代理程式一部分的客戶端點，以及我們的後端分析系統。

零時差保護非常重要

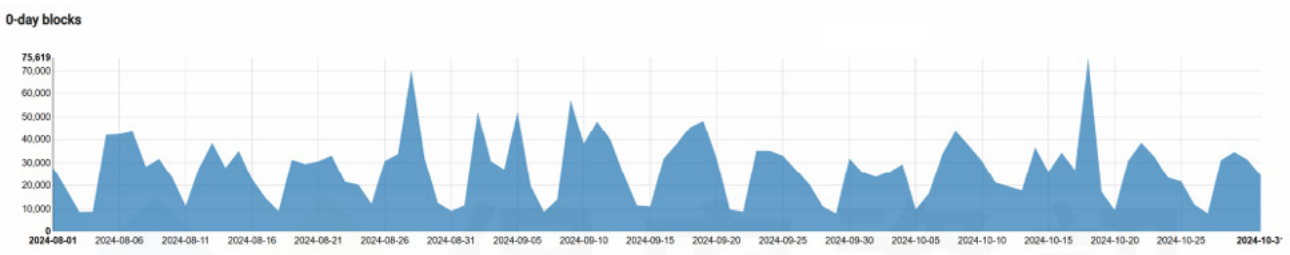
除了上述的分析平台之外，我們還運用雲端沙盒分析引擎 (Cloud Sandbox Analysis Engine)(非常適合的名稱「Cynic」)，執行多種 ML 模型和叢集演算法，根據威脅類型、潛在風險、動態和靜態元資料以及行為，對檔案進行分類和叢集。賽門鐵克利用自動化系統和人工的惡意軟體分析師盡快分析客戶提交的資料，並將情報擷取至 ML 訓練模型，以改善分類效能。我們的多模型進階機器學習技術可在 32 位元和 64 位元版本的各種檔案類型上執行，以提供可行的分析。當發現防護力有落差時，這些落差會由後端 ML 模型進行分析，並透過 Reputation lookups (信譽查詢) 迅速攔截。賽門鐵克進階機械學習的主要目標是防護全新的未知惡意軟體，也就是業界常說的零時差攻擊。這正是 ML 的優勢所在。

在上個季度，賽門鐵克的進階機器學習防護技術在賽門鐵克端點和閘道產品上攔截超過 1,800 萬個威脅。其中約有 260 萬個攔截是針對零時差攻擊，也就是我們的安全產品或防護技術從未見過的攻擊，這就是所謂「主動式」防護。與「被動式」防護不同，「被動式」防護是指針對攻擊增加新防護措施或更新現有的防護措施。主動式防護是對抗網路威脅的靈丹妙藥，也是各地潛在網路罪犯的剋星。

賽門鐵克進階機器學習防護技術在過去一個季度所提供的保護數據：

- 賽門鐵克 Advanced ML 在閘道產品上封鎖 1,240 萬個威脅
- 在端點上封鎖 580 萬個威脅
- 攔截 260 萬個零時差威脅，包括
  - 1 萬 6 千個勒索軟體 (HiddenTear、Gandcrab、Ryuk、Wannacry、Zombie、CryptoJoker、PureCrypter、Expiro 等)
  - 36 萬 5 千個 木馬程式 (Asprox, Cidox, BumbleBee, Cryect, CoinMiner, JokLoader, Nancrat, ToralDrop, WhisperGate, GenKryptik, AsyncRAT, Remcos, AgentTesla, Lokibot, LummaStealer, ZBot 等)
  - 11 萬個 Win32 (Babonock, Beapy, Cridex, Extrat, Qakbot, Fujacks, Wabot, Zorex, etc.)
  - 15 萬 5 千個 後門程式 (Wecoym、Rifelku、Matsnu、Ghostnet、Cobalt、Breut 等)
- 在端點封鎖 170 萬個瀏覽器型威脅--41% 來自 Chromium、28% 來自 MS Edge、8% 來自 Firefox
- 攔截 150 萬個嘗試從 USB 磁碟機等外部來源進入系統的威脅
- 在端點產品上封鎖 140 萬個透過命令列下載並執行惡意檔案的威脅
- 封鎖 13 萬 5 千 個使用點對點 (P2P) 網路程式下載的威脅，例如：Anydesk (RDP)、Utorrent 和 Bittorrent
- 封鎖 3 萬 7 千個 使用 SMB 進行網路檔案分享的攻擊
- 封鎖 9 千 300 個使用腳本主機 (WSH) (Powershell/cscript/wcript) 下載的威脅

在本季度內選擇端點和閘道的零時差保護措施



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。

欲深入瞭解賽門鐵克雲端沙盒分析引擎 (Cynic)，請點擊此處。

欲深入瞭解賽門鐵克的端點多層次防護解決方案中「進階機器學習」防護技術，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**。