賽門鐵克進階機器學習技術(AML)

2024 年 3 月 19 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

賽門鐵克進階機器學習技術 (AML) 是如何防範零時差威脅

機器學習 (通常簡稱為 ML) 是一種無特徵碼的技術，可在執行前階段阻止全新的惡意軟體。在賽門鐵克機器學習被應用在許多層面，以保護我們的客戶免受網路威脅。這些層級的設計目的是在我們的解決方案 (包括端點、閘道和我們的後端分析平臺) 看到可疑檔案、作業系統事件、登錄檔的機碼、網頁或網路活動的每個環節主動和被動地『把關』。賽門鐵克有能力利用一套全面的威脅掃描引擎，在新內容出現時立即對其進行動態分析，並將威脅情資同步到賽門鐵克全球威脅情資網路 (GIN：Global Intelligence Network)。賽門鐵克使用來自數百萬個端點的安全遙測資料、安全協力廠商提供的威脅相關資料以及海量的乾淨檔案集來訓練和評估各種 ML 模型。這些模型部署在眾多解決方案，用於檢測威脅，既包括作為我們代理一部分的用戶端點，也包括我們的後端分析系統。

零時差防護相當重要

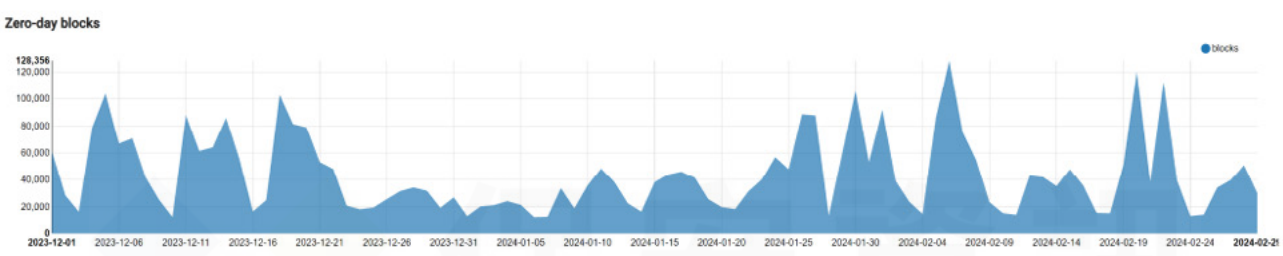
除上述分析平臺外，我們還利用 Cynic 雲端沙箱分析引擎 (以『Cynic』恰如其分的命名) 執行多個 ML 模型和叢集演算法，根據檔案的威脅類型、潛在風險、動態和靜態中繼資料 (metadata) 以及行為對檔案進行分門別類。賽門鐵克利用自動系統和人工惡意軟體分析師儘快分析客戶提交的檔案，並將分析結果輸入到 ML 訓練模型中，以提高分類效率。我們的多模型進階機器學習技術可在 32 位和 64 位版本的各種檔案類型上執行，以提供可付諸行動的分析。在發現防護漏洞時，後臺 ML 模型會對其進行分析，並透過信譽查詢立即阻止漏洞。賽門鐵克進階機器學習 (AML) 主要目標是防範全新的未知惡意軟體，即資安術語所說的零時差攻擊。這正是 ML 的優勢所在。

僅在上一季度，賽門鐵克的進階機器學習 (AML) 在賽門鐵克端點和閘道解決方案上攔阻將近 2,300 萬次威脅。其中約 390 萬次阻止的是零時差攻擊，也就是我們的任何安全產品或防護技術從未見過的攻擊。這就是所謂『主動』防護，而不是『被動』防護，後者是指針對攻擊增加新的防護措施或更新現有防護措施。主動防護是應對網路威脅的靈丹妙藥，也是各地網路犯罪分子的剋星。

在上一季度，賽門鐵克進階機器學習部分提供以下保護：

- 在閘道產品上，賽門鐵克進階機器學習攔截了 1,350 萬個威脅
- 在端點上封鎖了 930 萬個威脅
- 透過 ML 攔截了 390 萬個零時差威脅，其中包括
  - 9K 個勒索軟體 (Cerber、Cryptodefence、Gandcrab、Ryuk、Wannacry、Zombie 等)
  - 512K 個木馬程式 (Emotet、Cridex、Whispergate 等)
  - 160K 以『Win32.』開頭的威脅 (Qakbot、Fujacks、Expiro 等)
  - 230K 個後門 (Cobalt、Limitail、Berbew 等)
- 在端點上攔截了 110 萬個瀏覽器類型的威脅 -32% 來自 Chromium，24% 來自 MSEdge，15% 來自 Firefox
- 在端點產品上攔截了 73.1 萬個透過命令列下載和執行惡意檔案的威脅
- 攔截了 585K 次試圖從 USB 隨身碟等外部來源進入系統的威脅
- 阻止了 20 萬次使用伺服器訊息區塊 (Server Message Block，SMB) 網路傳輸協定進行網路檔案共用的攻擊
- 攔截了 105K 個使用點對點 (P2P) 網路程式 (例如：Anydesk (RDP)、Utorrent 和 Bittorrent) 下載的威脅
- 攔截了 5.9K 個使用腳本主機 (Powershell/csript/wcript) 下載的威脅

本季度在端點和閘道上的零時差防護圖表



欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。

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的雲沙盒分析引擎 (Cynic)，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**。