radware

Bot Manager Data Sheet

FORRESTER® Wave™: Leader, Q3 2018

Gartner Cool Vendor 2018

防止網站、手機 APP 和 API 的自動化攻擊

現今網路有超過一半的流量來自於機器人(Bot)，有些是合法的，有些則是惡意的。競爭對手常部署不同模式的“壞機器人”來實現其不當目的，包括帳戶接管、資料爬取、阻斷可用資產，以及發布阻斷服務(DoS)攻擊等，目的是竊取資料或導致服務中斷。傳統的緩解系統和策略通常無法檢測到複雜的大規模攻擊。透過專利半監督(semi-supervised)機器學習功能，Radware 的 Bot Manager 能跨管道進行精確的機器人管理，有效結合異常行為分析、集體機器人智能和設備指紋建立行為模型(behavior modeling)。

深度行為意圖分析 (IDBA)

透過專利半監督機器學習模組，準確辨識出有不良意圖的機器人。

完整防護 OWASP 自動化威脅 (OATs)

防止任何形式的帳戶接管、資產阻斷、DDoS、信用卡盜用和網頁抓取等威脅。

保護所有管道：網站、手機 APP 和 API

防禦鎖定各種數位資產的機器人 - 即使是專門攻擊多項資產的高端機器人。

非侵入式(Nonintrusive)方式

使用 API 或旁接模式進行高階擬人化機器人的實時檢測及阻擋，且完全不會對技術層面產生任何影響。

防止各種形式的威脅

帳戶接管

透過憑證填充(Credential Stuffing)和暴力攻擊(Brute Force)的方式登入、存取用戶帳號。

內容剽竊

詐騙者和第三方聚合器使用機器人抓取內容，並在幽靈網站上非法複製竊取的內容。

禮物卡詐騙

不法分子使用機器人來破解禮品卡，以辨識出有效的優惠券號碼和卡片代碼。

網路廣告詐騙

惡意機器人會在其發佈網站及手機 APP 上產生假的廣告，藉此累積非法點擊量。

應用程式 DoS 攻擊

應用程式 DoS 攻擊透過耗損系統資源、第三方 API、inventory 資料庫和其他關鍵資源的方式，降低網路應用程式的效能。

扭曲網站分析資料

產生網站資源上的自動化流量，使衡量指標被扭曲並誤導經營者的決策制定。

價格資料爬取

競爭對手在網站上部署機器人，竊取定價資訊，進而影響客戶購買決策。

產生垃圾郵件

惡意機器人透過垃圾帳戶、留言和假的註冊資料來淹沒線上市集和網路論壇。

主要特點

- **能用多種方式處理機器人流量**

  根據機器人特徵/類型制定行動，例如，餵送競爭者機器人假的定價和產品資料。Radware 將驗證碼(CAPTCHA)用於可疑的機器人上，利用封閉迴路回饋系統(closed-loop feedback system)中的訊號回饋將誤報數降至最低。

- **通透式(Transparent)報告及統整式分析**

  對搜尋引擎爬蟲和惡意機器人等不同類型的機器人進行細部分類和報告，以達到有效的流量管理。Radware Bot Manager 能和主要的分析平台無縫整合，包括 Google、Adobe Analytics 等。

- **易於整合**

  可透過各種彈性部署選項進行整合，包括 Radware 的 JavaScript tag、雲端連接器(Cloud Connector)或網頁伺服器(Web Server) plug-in 等；另外也可將虛擬設備用於整個網路應用程式或選定的範圍，輕鬆將 Bot Manager 部署到既有的基礎設施中。

- **DNS 無須重新導向**

  使用以 API 為基礎的解決方案來保護 Web 資產，且 DNS 無須重新導向，因此可以完全控管網頁應用程式、手機 App 和 API。

- **準確性和可擴充性**

  IDBA 深度行為意圖分析可過濾高階擬人化機器人而不產生誤報，同時維持網站功能和用戶體驗的水準。Bot Manager 運用尖端技術，即使在網路流量的高峰，也能保有良好的可擴充性。

- **充分管理的服務**

  Bot Manager 也可與 Radware Cloud WAF 整合為安全服務，提供應用程式 360°的完整保護。

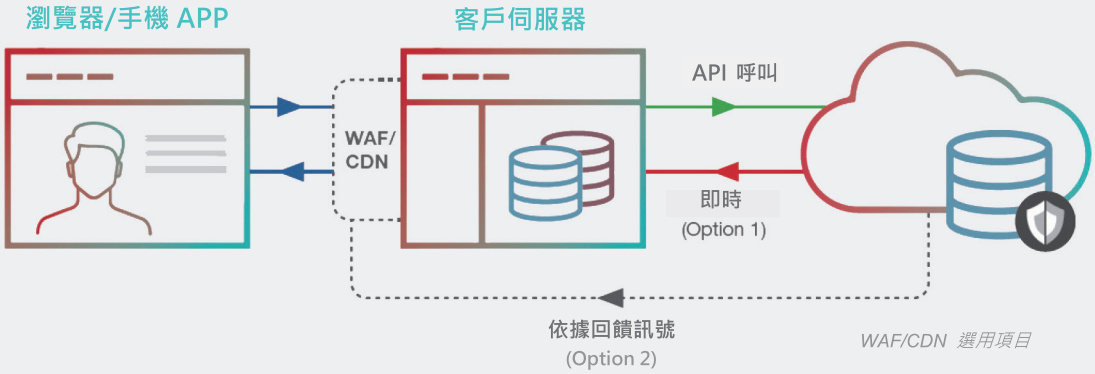

圖 1：Radware Bot Manager 運作方式

Radware 攻擊緩解解決方案

Radware Bot Manager 結合 Radware 攻擊緩解解決方案（AMS），可提供業界最先進的防禦，防止複雜的自動化攻擊。Radware 的解決方案透過充分整合的系統，提供完整的網路和應用程式安全防護，可同步本地端和雲端的解決方案，保護企業組織免於各種攻擊，如網頁應用程式攻擊、阻斷服務、惡意機器人和進階惡意軟體。Radware AMS 具有通過驗證、受專利保護的機器學習功能、先進的自動化和實時情報共享，可在最小化延遲與誤報的同時，實現最大化的安全性。