CLOUDFLARE

白皮書

惡意機器人應對手冊：預警信號及其處理方法

目錄

介紹

如今，機器人佔網路流量的 30% 左右——而且其中許多機器人的目的在於破壞像您這樣的組織，估計其中 93% 的機器人流量未經驗證，並且可能具有惡意。內容和價格剽竊、帳戶盜用、認證與信用卡填充、庫存囤積，以及殭屍網路驅動的分散式阻斷服務 (DDoS) 攻擊日益普遍，表明惡意機器人執行者正變得越來越複雜和老練。

此外，傳統的反機器人措施，例如位置封鎖、IP 位址封鎖和傳統 CAPTCHA，如今已不再有效。事實上，機器人解決 CAPTCHA 比人類更容易[1]。

因此，任何單一策略都無法阻止所有機器人，也無法防止機器人損害您的使用者和品牌。唯一有效的方法是對各種機器人警告信號保持警惕，並在收集資料後部署針對性回應、模式偵測、預測性分析和其他輔助策略來逐一應對。

1. https://www.usenix.org/conference/usenixsecurity23/presentation/searles

機器人問題的警告信號

透過追蹤一系列潛在信號，您有很大機會在惡意機器人造成嚴重破壞前發現它們。如下是需要注意的信號：

基礎架構成本上升，但業務量毫無增長

您網站的所有流量都會產生一定的費用。無論是誰或任何應用程式存取您的內容，您都必須承擔儲存和運算的費用。但是惡意機器人可能會增加與流量相關的成本，而不會給您的業務帶來任何收入。雖然搜尋引擎使用善意機器人來索引您網站上的內容，從而提升您的 SEO 排名，但惡意機器人每年都會產生大量的頻寬費用。

針對數量少、需求高庫存的異常購買

如果您發現向極少一部分買家出售的庫存比例高得可疑，罪魁禍首可能就是庫存囤積機器人。雖然其中一些機器人會簡單地填充並捨棄購物車以封鎖合法客戶，但其他機器人會真正購買您的庫存，以便在其他網站上以更高的價格轉售。

客戶投訴增加

與帳戶鎖定和詐騙交易有關的支援工單數量上升，可能是認證填充機器人的跡象。這些機器人會使用從過去的洩漏事件中收集的資訊，來盜用合法的使用者帳戶。這些詐騙交易不僅會對您的客戶體驗造成負面影響，還會使伺服器過載，從而導致頁面載入時間變長，甚至使您的網站無法使用。

登入嘗試失敗次數增加

每個客戶都會時不時地輸錯密碼，但是，如果您發現登入嘗試失敗的次數突然增加，那很可能是遇到了機器人問題。雖然一些認證填充機器人試圖透過竊取的認證來存取合法的客戶帳戶，但一種更簡單、更常見的技術是發起暴力攻擊，在這種攻擊中，機器人會使用數以千計的常見使用者名稱和密碼字典嘗試進行多次快速登入。當機器人超出您網站對特定帳戶的登入失敗次數限制時，該帳戶真正的人類所有者將被鎖定，直到您解決該問題，這是一個重大的使用者體驗難題。

廣告支出收益低

數位廣告是增加網站流量的有效手段，但對惡意機器人而言，這也是一種賺錢的工具。許多流量機器人模仿人類使用者的行為，反覆點選廣告以推高點選付費 (PPC) 支出，然後離開頁面而不購買。儘管某些廣告平台已經部署機器學習演算法來減少點擊詐騙，但很多此類行為仍未發現[2]。
因此，採取主動並監測對廣告的每一次點擊至關重要。

頁面瀏覽量分析失真

如果您的網頁瀏覽量突然無緣無故飆升，有可能是惡意機器人在作祟。如果您剛剛推出新產品或舉行促銷活動，則激增的流量可能來自人類使用者，但惡意機器人操作者正變得越來越聰明，他們會在此時部署內容剽竊機器人來竊取您的內容，並對您的綜合分析資料產生負面影響。

帳戶建立量突增

如果突然出現成百上千的新使用者帳戶，機器人可能是幕後黑手。惡意機器人可以使用這些虛假的帳戶在您的公眾評價系統中濫發資訊，並進行其他多種形式的詐騙，這不僅會威脅您的收入和使用者留存率，還會威脅到您的品牌信譽。

在未經批准的網站上複製您的內容

其他網站分享您的內容可能是好事，但是完全相同的內容激增可能表示內容剽竊機器人正在運作。這些機器人會竊取您費時費力整理和組織的資訊，讓惡意網站營運者得以在其自有網域上發佈這些內容，增加其流量並對您的網站造成打擊。

來自異常地理位置的流量

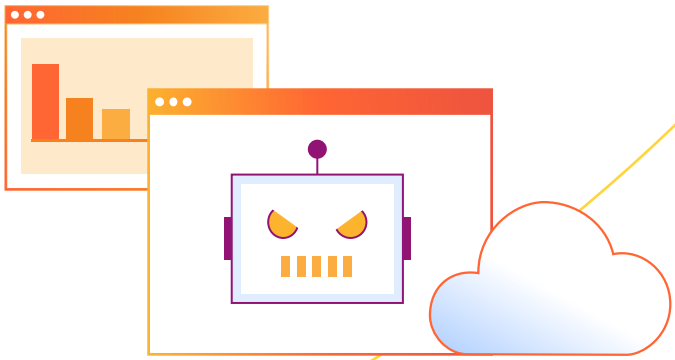
來自意外位置的流量暴增可能表明有惡意機器人在活動，如果這些活動密集出現，並集中在您的客戶沒有居住或您的服務不可用的地區，則可能性更大。請密切關注與您的一般使用者群體無關的任何可疑活動。

在異常時段出現來自常見位置的流量

就像來自意外位置的流量暴增可能表示有惡意機器人一樣，在異常時段來自正常位置的流量激增也可能表示機器人試圖偽裝成您的一般使用者。例如，如果您在半夜看到某個常見地區的活動量激增，您可能需要更仔細地調查這些流量。

信用卡驗證失敗次數增加

一個特別危險的惡意機器人跡象是驗證失敗的信用卡交易數量增加。信用卡填充機器人會測試成千上萬個被盜的信用卡號碼，試圖找到可用的卡號。其做法是在安全性較低的網站上購買低價值物品，然後在較大型的網站上進行較大宗交易，或在暗網上出售經過驗證的卡號。您的網站可能在上述過程中的任一環節被加以利用。如果交易失敗的情況比較嚴重，您的付款服務提供者可能會對您施加罰款。



2. https://www.entrepreneur.com/article/313943

對抗機器人的策略

由於每一個機器人攻擊都不盡相同，您通常需要同時使用多種策略，才能成功阻止全部惡意機器人。請考慮如下策略：

發現惡意機器人後立即攔截

針對機器人，最不言而喻、也最有效的對策之一：直接封鎖您確定為來自惡意機器人活動的所有流量。僅此一項策略就可以為您節省大量的頻寬和儲存成本，更不用說維護消費者的信任以及品牌聲譽了。同時，請記住，如果機器人操作者具有很強的動機，他們可能會改變策略，並使用不同的攻擊策略捲土重來。

將您知道的所有善意機器人列入允許清單

在您偵測和封鎖惡意機器人的同時，確保來自搜尋引擎和合作夥伴的善意機器人仍然能夠抓取您的網站內容至關重要。這不僅可以確保您的 SEO 排名保持穩定，還能使第三方服務引薦給您的合法客戶流量順暢流動。列入允許清單還會使設定機器人封鎖規則變得更加輕鬆，這些規則不會對真正的人類訪客產生負面影響。

對您偵測到的可疑機器人進行查問

一旦注意到可疑登入、低頁面深度或短頁面停留時間、信用卡驗證失敗或任何其他標誌性機器人行為模式，就必須部署安全性測試。過去，人們認為傳送 CAPTCHA 查問是一種最佳做法。不過，許多進階機器人現在能比人類使用者更快、更準確地解開這些謎題。

目前最好的方法是使用無需 CAPTCHA 的查問方式，其中「查問」軟體會考量多種因素，以判斷使用者是否為機器人（例如網路、裝置、JavaScript 指紋）。
理想情況下，這類「無 CAPTCHA」查問最好與完整的機器人管理解決方案整合，以達到最高的準確性（詳情請參閱「結論」）。

限制使用者請求資訊的速度

限速能有效封鎖不太複雜的機器人。對任何 IP 位址可以向您的網站提交請求的次數設定硬性限制，藉此可以防止許多簡單的暴力機器人攻擊（這些攻擊會試圖使用成千上萬的字典單詞和常用密碼進行登入）。然而，當今更進階的機器人可以將其請求數保持為略低於您的限速，從而在不被發現的情況下繼續進行破壞。

保留所有網站流量的詳細記錄

儘管您可能已經維護了每日頁面瀏覽量和帳戶登入記錄，但更詳細的使用者資訊記錄（例如 IP 位址、瀏覽器、裝置、作業系統、地理位置、引薦來源網址、網路和頁面瀏覽量）對於偵測更細微的活動模式而言具有無可估量的價值。記錄可以讓您清楚地瞭解機器人在網站上的行為方式，從而使您可以設定更有效的安全性策略。此外，在您確實遭受資料外洩的情況下，記錄對於報告和合規性往往至關重要。

將機器人重新導向到替代內容

如果您有相當把握認為某個流量來源是機器人，可對此提供替代內容，以消耗其計算資源。您甚至可以將虛假資料（例如錯誤的定價資訊）提供給內容剽竊機器人，使它們對操作者毫無用處。諸如此類的技術將使您有時間觀察每個機器人的行為，瞭解其活動模式，並制定徹底解決的策略。

要求所有使用者進行額外驗證

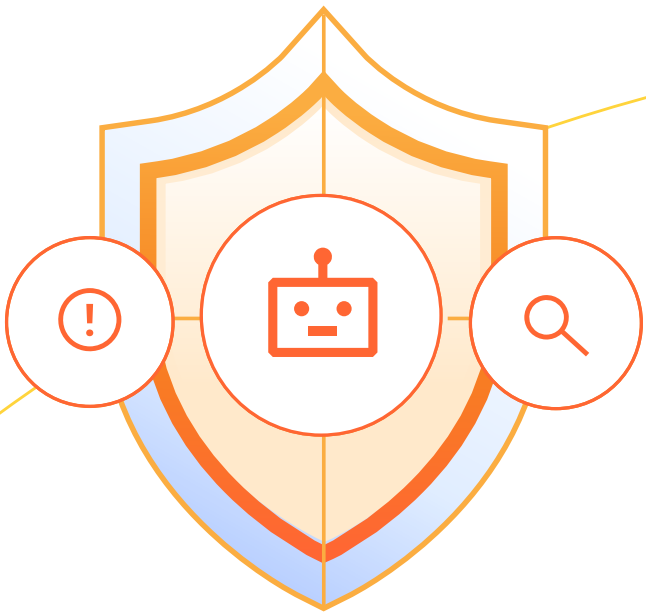
隨著機器人攻擊日益普遍，越來越多的網站加強了安全性措施，即使對於合法的人類登入也是如此。例如，雙重驗證 (2FA) 要求使用者在多個裝置或帳戶上確認其身分，而一次性密碼 (OTP) 則可以使帳戶更難破解，藉此封鎖認證填充機器人。但是請記住，這些技術會導致登入流程不太順暢，可能會對您的使用者體驗產生負面影響。

結論

在研究這些策略時，請記住：單獨使用其中任何一種方式都無法封鎖所有機器人。為了保護您的業務，您可能需要結合使用各種策略，並引入進階的多變數模式分析。Cloudflare Bot Management 可以幫助各行各業的組織採用這種多管齊下的方法。它已整合到更廣泛的 Cloudflare 網路中，該網路支援數百萬個網際網路內容，覆蓋全球 330 多座城市。

透過利用來自整個網路的持續威脅情報，Cloudflare Bot Management 提供行為分析、機器學習和用戶端指紋識別功能，從而在打擊惡意機器人時節省大量精力。此外，Cloudflare 還提供 Turnstile，這是一種近乎無感的、無需 CAPTCHA 的機器人查問機制，只需幾行程式碼即可整合至任何 Web 應用程式。

進一步瞭解 Cloudflare Bot Management。



+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

REV:BDES-6333.2024SEPT03