radware

Bot Manager Adatlap

Gartner Cool Vendor 2018

Akadályozza meg a weboldalak, mobil appok és API-k elleni automatizált támadásokat

Az összes internetes forgalomnak több mint a felét botok generálják — ezeknek egy része legitim, másik része rosszindulatú. A versenytársak és az ellenfelek is gyakran telepítenek „rossz” botokat, amelyek különféle módszereket használnak becstelen célok elérése érdekében. Ezek közé tartozik az account-rablás, az adat scraping, a készletmegtagadási és DoS támadások adatlopási vagy szolgáltatáslassítási célzattal. A kifinomult, nagyszabású támadások gyakran rejtve maradnak a hagyományos védelmi rendszerek és stratégiák előtt. Szabadalmaztatott, részlegesen felügyelt gépi tanuló képességek használatával a Radware *Bot Managere* lehetővé teszi a precíz bot menedzsmentet a weben, mobilapplikációkon és alkalmazásprogramozási felületeken (API-kon), kombinálva a granuláris szándékelemzés viselkedési modellezését, a kollektív bot információszerzést, és az eszközök ujjlenyomat-vételét.

SZÁNDÉK-ALAPÚ VISELKEDÉSI MÉLYELEMZÉS (IDBA)

Azonosítsa a legnagyobb precizitással a botok szándékait a szabadalmaztatott, részlegesen felügyelt gépi tanuló modellek segítségével

OWASP AUTOMATIZÁLT TÁMADÁSOK TELJESKÖRŰ LEFEDÉSE

Védekezzen az account-rablás, a készletmegtagadás, a DDoS támadás, a bankkártyacsalás és a web scraping miden formája ellen

VÉDJEN MEG MINDEN CSATORNÁT: WEB, MOBIL APP ÉS API-K

Védekezzen azon botokkal szemben, amelyek különféle digitális eszközöket vesznek célba – legyen szó akár egyszerre többfajta eszköz megtámadására tervezett kifinomult botokról

RUGALMAS INTEGRÁCIÓS LEHETŐSÉGEK

Nem intruzív telepítés SDK, web szerver vagy tartalomelosztó hálózat (CDN) pluginek, JavaScript (JS) tag vagy fordított proxy használatával – nem növeli a technológiai infrastruktúrát

Védelem a veszélyek széles skálájával szemben

Account-rablás
A felhasználói adatokkal történő visszaélések és a brute force támadások célja a jogosulatlan hozzáférés az ügyfélprofilokhoz.

Ajándékkártya-csalás
A kártyacsalók botokat használnak az ajándékkártyák feltörésére és az érvényes kupon- és utalványkódok beazonosítására.

Alkalmazás DoS
A szolgáltatásmegtagadással járó támadások rontják a web-alkalmazások teljesítményét, mivel kimerítik a rendszer erőforrásait, az API-kat, az adat-bázisokat és más kritikus erőforrásokat.

Ár scraping
A versenytársak az Ön weboldalán olyan botokat telepítenek, amelyek ellopják az árinformációkat és befolyásolják az ügyfelek vásárlási döntéseit.

Tartalom scraping
A csalók és a külső aggregátorok botokat használnak arra, hogy begyűjtsék a tartalmakat és illegálisan lemásolják őket a szellem weboldalakra.

Hamis hirdetések
A rosszindulatú botok hamis impression-öket és átkattintásokat generálnak a hirdető weboldalakon és azok mobil appjain.

Torz analitika
Az Ön webes felületein átfolyó automatizált forgalom torzítja az adatokat és félrevezeti a döntéshozókat.

Űrlap spam
A rosszindulatú botok kéretlen adatokkal, kommentekkel és álregisztrációkkal árasztják el az online boltokat és közösségi fórumokat.

RelNet technológia
1047 Budapest, Váci út 71.
Tel: +36 (1) 48 48 300
https://relnet.hu
kereskedelem@relnet.hu

Fő jellemzők

- **A bot forgalom kezelése többféleképpen** — A műveletek az adott bot szignatúrája vagy típusa szerint vannak beállítva, például a versenytársak botjai hamis árakat és termékinformációkat kapnak. A Radware bot gyanú esetén CAPTCHA-t használ, miközben a válaszokat egy zárt láncú visszajelzés (closed-loop feedback) rendszerbe helyezi a hamis pozitív jelzések minimalizálása érdekében.

- **Átlátható riportolás és átfogó elemzés** — A különböző bot típusok – például kereső botok, rosszindulatú botok – granuláris osztályozása és riportolása hatékony adatforgalom-kezelést tesznek lehetővé. A Radware *Bot Managere* zökkenőmentesen integrálható a vezető analitikai platformokkal, beleértve a Google-t és az Adobe Analyticsot.

- **Egyszerű integráció** — A rugalmas telepítési opciók közé tartozik a JS tag-en, felhő csatlakozókon és webszerver plug-ineken keresztüli integráció. Vagy egy virtuális eszköz is rendelkezésre áll az egész webapplikáció vagy annak kiválasztott részei számára. A Radware API-alapú megközelítésének használatával a DNS-átirányítás nem kötelező, így a meglévő alkalmazáshalmazba történő telepítés egyszerű és zökkenőmentes.

- **Pontosság és skálázhatóság** — Az IDBA kiszűri az igen kifinomult emberszerű botokat, hamis pozitív jelzések okozása nélkül. A weboldal funkcionalitása és a felhasználói élmény érintetlen marad. A Radware *Bot Managere* élvonalbeli technológiák bevetésével tartja fenn a nagyfokú méretezhetőséget a hálózati csúcsforgalomban is.

- **Teljeskörűen menedzselt szolgáltatás —** A Radware *Bot Manager* a Radware Cloud webalkalmazásszintű tűzfalával (WAF) integrálva biztonsági szolgáltatásként is elérhető a teljes, 360 fokos alkalmazásvédelem érdekében.

- **Dedikált API-védelem —** A navigációs áramlás ellenőrzése és az M2M-kommunikáció ujjlenyomatvétele, annak érdekében, hogy elkerülhető legyen a rosszindulatú botok által célba vett API-k meghívása.

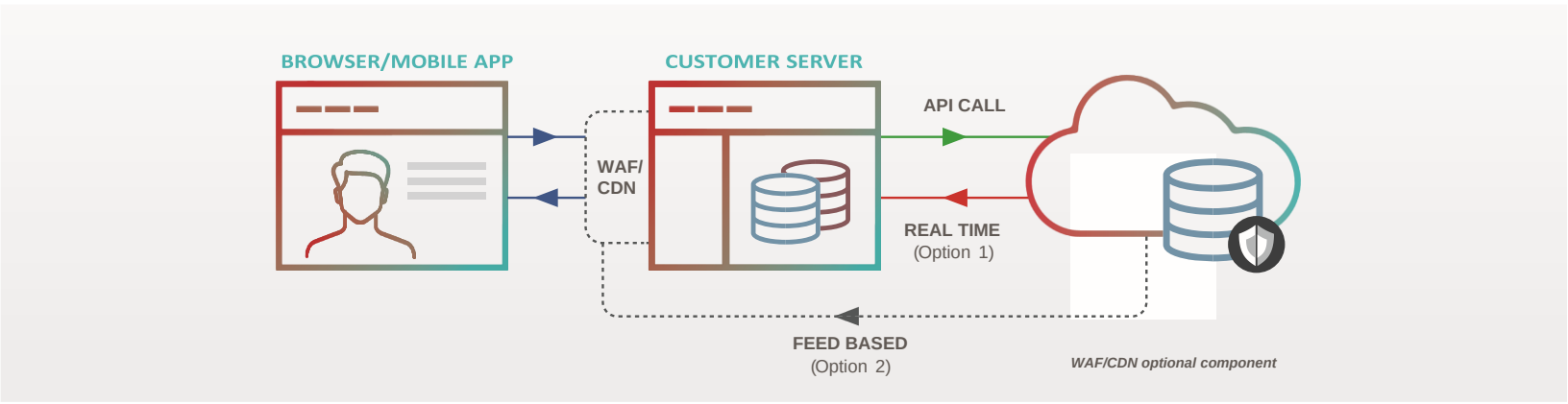
API-védelem a rosszindulatú botok ellen

API forgalomszabályozás
M2M és IoT-védelem

Meghívási kontextus Web és mobil API védelem

API-kliens SDK
Egyedi forrásazonosítás az M2M-kommunikáció biztosítása érdekében

Hitelesítési folyamat
Accountrablás-védelem API-k számára a sikertelenül bejelentkező forrásokkal szemben



1. ábra: A Radware Bot Manager munkafolyamatának diagramja

- **Teljes Alkalmazásbiztonsági termékcsoport —** Magában foglalja a WAF-ot, a bot menedzsert, az API-biztonságot és a DoS-védelmet, amelyek együttesen a legrobusztusabb alkalmazásvédelmet nyújtják.

A Radware teljes alkalmazásbiztonsági termékegyüttese

A Radware az iparág legfejlettebb alkalmazásvédelmét kínálja WAF-fal, Bot menedzserrel, API-védelemmel és DDoS elhárítással. A Radware megoldásai teljeskörű hálózat- és alkalmazásvédelmet biztosítanak a helyszínen és a felhőben egyaránt. Sokféle veszéllyel szemben védjük a szervezeteket, mint például az injekció, a 'cross-site scripting' (XSS), a jogosulatlan hozzáférés, az account rablás, a web scarping vagy a szolgáltatásmegtagadás. A Radware bizonyított, szabadalmaztatott gépi tanuló képességeket, fejlett automatizációt és valós idejű információmegosztást kínál a maximális biztonság érdekében, minimális hamis pozitív jelzéssel és látenciával.