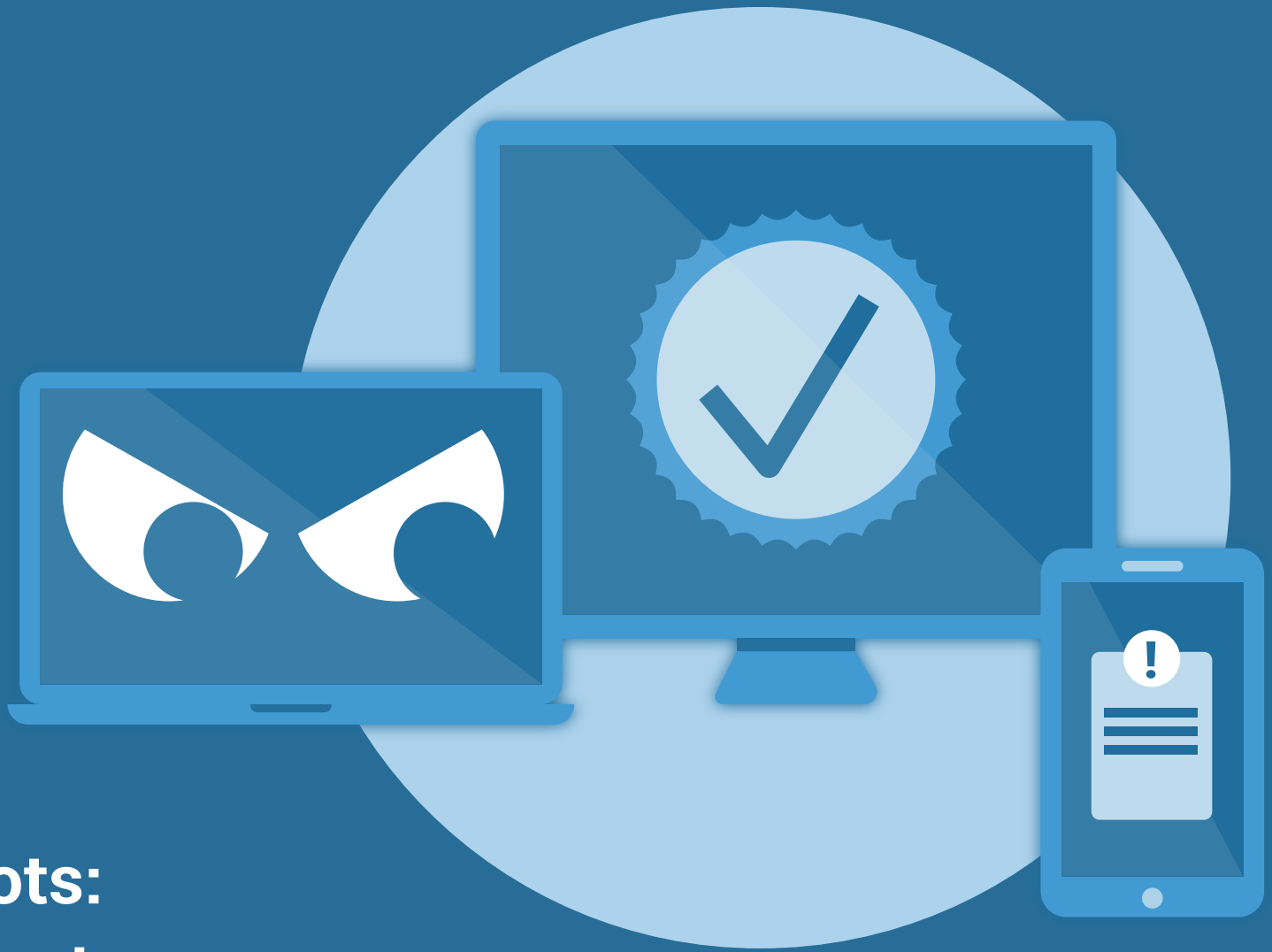


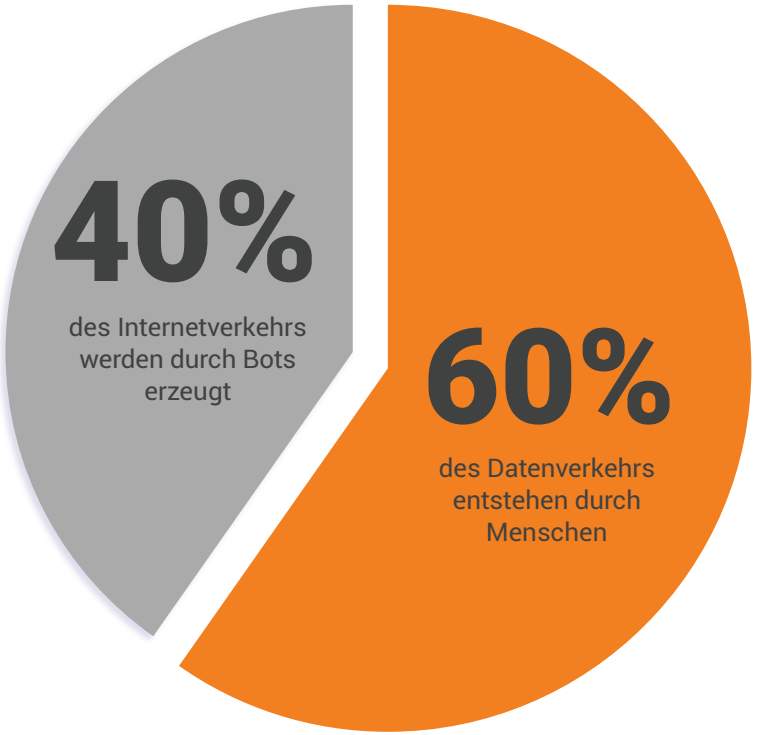
Schädliche Bots: die fünf häufigsten Irrtümer

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

CLOUDFLARE®

Inhalt

Irrtümer über bösartigen Bot-Verkehr

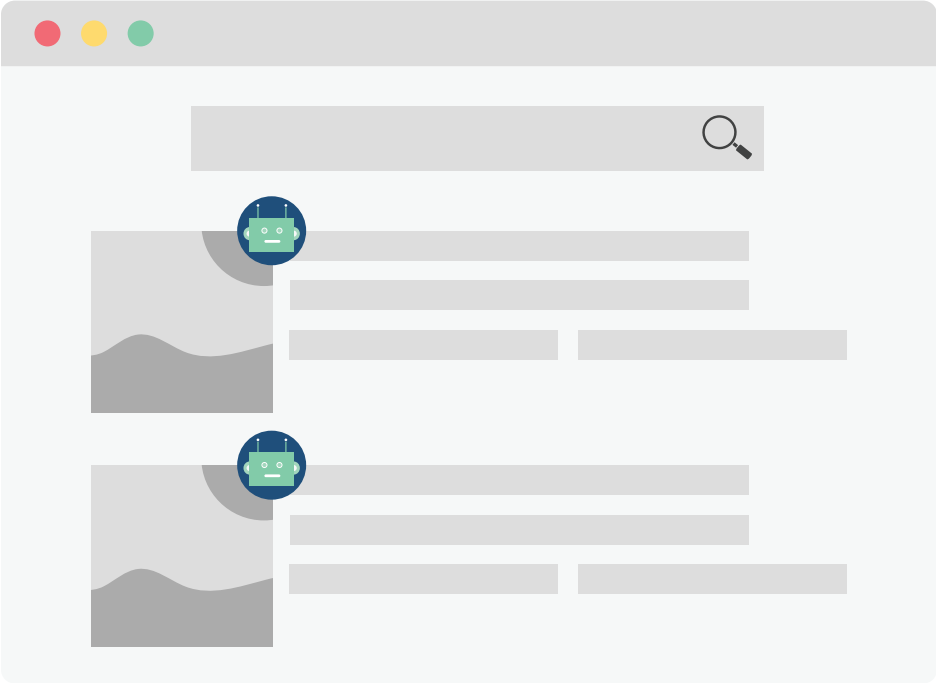


Bis zu 40 % des heutigen Internetverkehrs werden von Bots generiert[1] – und leider haben viele dieser nicht menschlichen Nutzer von Websites und Apps nichts Gutes im Sinn. Angesichts der wachsenden Verbreitung und Raffinesse bösartiger Bots ist es nicht immer leicht, Fakt und Fiktion klar voneinander zu trennen. Das erschwert Unternehmen die Abschätzung der Risiken und behindert die Suche nach wirksamen Gegenmaßnahmen.

Um für mehr Klarheit zu sorgen, nehmen wir einige der häufigsten Fehlannahmen unter die Lupe und erläutern, wie sich ein Unternehmen mit einem gut fundierten Ansatz bösartige Bots vom Leib halten kann.

IRRTUM 1

„Alle Bots führen Böses im Schilde“



Auch wenn schädliche Bots normalerweise die größte Aufmerksamkeit erhalten, sind gutartige Bots fast genauso stark verbreitet.

Sie tragen entscheidend dazu bei, das digitale Geschäft aufrecht zu erhalten. Bots unterstützen beispielsweise Unternehmen wie Google, Bing und Baidu bei der Indexierung von Milliarden von Websites, damit diese in Suchergebnissen auftauchen. Bei jeder Suchanfrage auf Reiseportalen wie Expedia oder Priceline greifen ganze Teams von Partner-Bots auf die Websites von Lufthansa, British Airways und anderen Fluggesellschaften zu, um die den Suchkriterien entsprechenden Flugzeiten und -preise auszulesen und aufzulisten.

Weiter >>

Die Rolle gutartiger Bots

Diese Unterscheidung ist deshalb so wichtig, weil gute Bots für das moderne Internet eine so große Bedeutung haben, dass das Blockieren sämtlicher nicht menschlicher Nutzer zur Abwehr bösartiger Bots keine praktikable Lösung ist.

Angreifer sind sich dieser Tatsache sehr wohl bewusst. Deshalb imitieren sie bei der Programmierung ihrer schädlichen Programme gezielt das Verhalten gutartiger und für die Unternehmen vorteilhafter Bots. Scraper-Bots beispielsweise sind in der Lage, die Eigeninhalte einer Website zu kopieren und unerlaubt auf den Sites von Betrügern zu veröffentlichen. Wer aber undifferenziert alle Scraper blockiert, nimmt in Kauf, dass auch wohlgesonnene Akteure wie Vertriebspartner oder Bewertungsseiten ausgesperrt werden. Diese können dann nicht mehr auf die Informationen zugreifen, die sie benötigen, um rechtmäßig für Unternehmen zu werben.

> *Vor der Einführung von Cloudflare tappten wir einfach im Dunkeln. Wir hatten keine Vorstellung davon, wie groß der Anteil der durch Bots erzeugten Zugriffe auf unsere Infrastruktur war und ob wir im Interesse unserer Verlagspartner Abwehrmaßnahmen gegen bösartigen Traffic ergreifen sollten.“*
>
> **Romeo Ju** Präsident
>
> **Sulvo**

IRRTUM 2

„Bots nehmen nur die E-Commerce-, Reise- und Finanzbranche ins Visier“

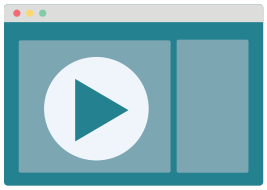
Viele aufsehenerregende Bot-Angriffe richten sich zwar gegen Banken, Fluglinien, Hotels und E-Commerce-Unternehmen, doch zunehmend geraten auch viele andere Branchen ins Fadenkreuz dieser Schadprogramme. Schon seit mehreren Jahren lässt sich beobachten, dass Bots auch auf Gesundheits- und Bildungseinrichtungen, Ticketanbieter, Unternehmen aus der Spiele- und Werbeindustrie, Marketingfirmen, Verlage und selbst Behörden angesetzt werden.

Je nach Branche wenden Bot-Betreiber dabei die unterschiedlichsten Strategien an. Viele Bot-Angriffe sind sogar ganz individuell auf die Schwachstellen in der Geschäftslogik eines bestimmten Unternehmens zugeschnitten. Eine Website, die Inhalte für Millionen externer Nutzer bereitstellt, kann zum Beispiel einem Content Scraping- oder Inventory Hoarding-Angriff zum Opfer fallen. Ein Anbieter, der sensible interne Daten speichert, ist dagegen unter Umständen Brute Force-Attacken ausgesetzt, die auf das Knacken von Passwörtern abzielen.

Tatsächlich kann jede Website mit einer Login-Seite für Kunden ein attraktives Ziel für bösartige Bots darstellen. Und große digitale Dienstleister, etwa im Bereich Marketing, IT oder Webdesign, können auf einen Bot-Betreiber mit bösen Absichten ebenso anziehend wirken wie ein Banktresor voller Geldbündel.

IRRTUM 3

„Bot-Angriffe treten am häufigsten während des Feiertagsgeschäfts auf“



An Feiertagen wird ohne Zweifel eine große Anzahl von Bot-Angriffen registriert.[2] Zur Wahrheit gehört aber auch, dass man das ganze Jahr über mit solchen Attacken rechnen muss. Ein möglicher Anlass sind Großereignisse wie die Markteinführung eines neuen Produkts, aber es gibt auch Auslöser, die sich deutlich schwieriger vorhersagen lassen.

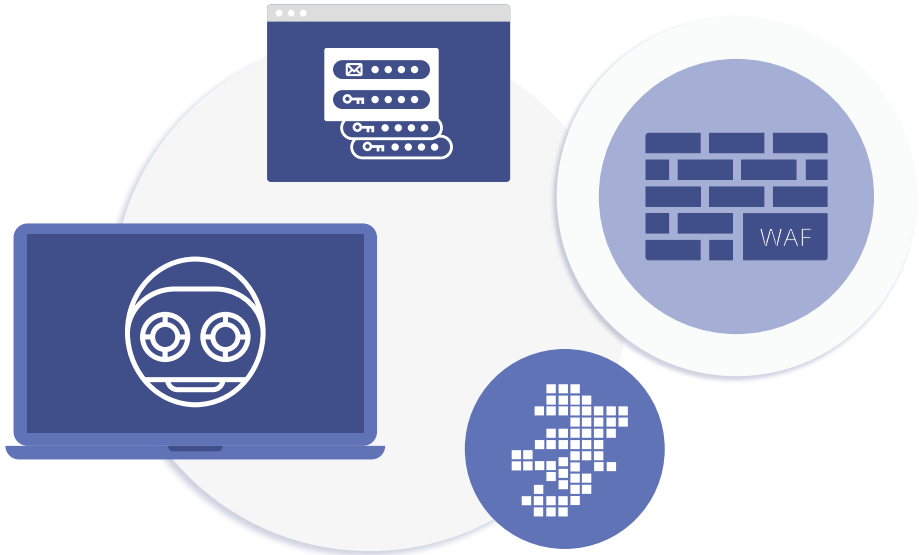
▶ Bot-Angriffe sind ein ganzjähriges Phänomen

Zum Beispiel sorgte im November 2019 ein arglistiger Bot-Angriff auf Disney zum Start der neuen Streaming-Plattform Disney+ für Schlagzeilen:[3] Angreifer nutzten die Einführung des Dienstes, um mit Credential Stuffing Kundenkonten ins Visier zu nehmen. Im Anschluss daran wurden Tausende dieser kompromittierten Konten im Dark Web zum Verkauf angeboten. Die Kriminellen, die diese Zugangsdaten erworben haben, kennen nun womöglich nicht nur die Bankverbindung der betroffenen Nutzer, sondern auch deren Login-Informationen für viele andere Websites und Anwendungen.

Ähnlich schwere Sicherheitsvorfälle wie der Angriff auf Disney gab es zwar in jüngster Zeit eher selten, aber es vergeht kein Monat, in dem es nicht zu zahlreichen kleineren Attacken kommt. Und die völlige Unvorhersehbarkeit dieser bösartigen Aktivitäten – man denke etwa auch an den Credential Stuffing-Angriff auf J.Crew vom April 2019[4] – ist eines der überzeugendsten Argumente für eine Lösung zur Bot-Abwehr, die an mehreren Stellen ansetzt.

IRRTUM 4

„Man kann alle schädlichen Bots mit einem einzigen Tool abwehren“



Auf den ersten Blick könnte man meinen, dass bereits eine Methode genügt – sei es DDoS-Abwehr, Durchsatzratenbegrenzung, eine Web Application Firewall (WAF), Multi-Faktor-Authentifizierung oder auch CAPTCHAs –, um die Anforderungen eines Unternehmens im Bereich Bot-Management zu erfüllen. Doch die Wirklichkeit sieht anders aus: Bot-Angriffe werden immer raffinierter und können durch das Nachahmen menschlichen Verhaltens individuelle Abwehrmechanismen überwinden. Unternehmen kommen um eine umfassende Bot-Management-Lösung nicht herum.

Weiter >>

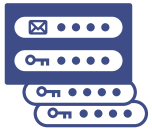
DDoS-Abwehr kann ein wirksames Mittel gegen volumetrische Angriffe sein. Dabei versucht ein Botnet, durch einen hohen Internet-Traffic einen Server, einen Dienst oder ein Netzwerk beziehungsweise die sie umgebende Infrastruktur zu überlasten und so eine Störung zu verursachen. Weitaus weniger geeignet ist dieses Tool aber, wenn es um das Aufspüren individueller Bots geht, die einen menschlichen Nutzer nachahmen.

Durchsatzratenbegrenzung kann einfache Bot-Angriffe blockieren, die eine übermäßige Anzahl von Anfragen generieren. Doch raffinierteren Bots gelingt es, unter dem Radar zu bleiben, indem sie einfach die Zahl ihrer Anfragen einschränken. Viele der modernen bösartigen Bots agieren unauffällig, indem sie eine Aktion nur so schnell und häufig wiederholen, wie das auch ein Mensch tun würde.

WAFs bieten Schutz vor SQL-Injections, Cross-Site Scripting (XSS) und Zero Day-Angriffen, indem sie Regeln anwenden, die Zugriffe von bestimmten IP-Adressspannen oder geographischen Standorten blockieren. Bot-Betreiber können heute allerdings zwischen Millionen von IP-Adressen in Hunderten Ländern wechseln.

Bot-Erkennung mittels JavaScript kann den Zugriff über unzulässige Browser unterbinden. Doch leider schränken JavaScript-basierte Testaufgaben für Bots auch die Website-Performance ein, weil die Anwendung jede Anfrage beim Anbieter überprüfen muss, was die Endnutzererfahrung beeinträchtigt. Zudem stellt die Implementierung die IT- und Sicherheitsabteilungen von Unternehmen vor eine Herausforderung, weil externe JavaScript-Bibliotheken verwaltet und abgesichert werden müssen.

CAPTCHAs können sich als effektiver Baustein bei der Bot-Abwehr erweisen, indem sie offenkundig bösartige Bots aufspüren. Allerdings sind einige Bots der neuesten Generation dazu fähig, CAPTCHA-Aufgaben zu lösen. Außerdem beeinträchtigen CAPTCHAs in jedem Fall die Nutzererfahrung, weil sie unnötige Irritationen beim Login und Einkaufsvorgang verursachen.



Multi-Faktor-Authentifizierung (MFA) kann zum Schutz vor nicht autorisierten Logins beitragen, wenn Bots versuchen, Anmeldedaten von legitimen Nutzern zu verwenden. Bei den meisten Anwendungsfällen, bei denen Bots zum Einsatz kommen, geht diese Lösung jedoch ins Leere. Zudem stört auch dieser umständliche Prozess die Nutzererfahrung.

IRRTUM 5

„Bot-Angriffe sind so vielfältig, dass jeder seine eigene Bot-Management-Lösung entwickeln sollte“

Angesichts der raffinierten Angriffe moderner Bots, die nicht selten genau auf ein konkretes Ziel abgestimmt sind, mag die Entwicklung einer eigenen Bot-Management-Lösung auf den ersten Blick als die beste Abwehrstrategie erscheinen.
Kurzfristig kann sich eine unternehmensintern konzipierte Lösung auch durchaus als hocheffektiv erweisen, doch ein dauerhafter Schutz setzt voraus, dass sich firmeneigene Fachleute um kostspielige Wartungsarbeiten und lästige Upgrades kümmern.

Erschwerend kommt hinzu, dass bösartige Bots sich nach jeder gescheiterten Attacke anpassen: Sie ändern ihre Angriffsmuster, verfeinern ihre Nachahmung menschlicher Nutzer und lernen auf diese Weise, auch den ausgefeiltesten Sicherheitstools der heutigen Zeit ein Schnippchen zu schlagen. Um bösartigen Bots immer einen Schritt voraus zu sein, müsste man deshalb bei einer individuell konzipierten Lösung die Regeln und Richtlinien der Bot-Abwehr ständig nachjustieren.

Und schließlich bliebe auch die ausgeklügeltste firmeninterne Bot-Lösung auf sich gestellt: Man könnte Bot-Angriffe nur noch anhand eigener interner Daten vorhersagen und verdächtige Aktivitätsmuster lediglich mit veralteten Algorithmen analysieren. Eine maßgeschneiderte Lösung würde deshalb viele Fehlalarme verzeichnen und damit die Erfahrung legitimer Nutzer beeinträchtigen.

Fazit: So sieht die ideale Lösung für das Bot-Management aus

Eine effektive Bot-Management-Lösung sollte die besten Eigenschaften aller oben aufgeführten Werkzeuge und Ansätze auf sich vereinen. Sie sollte globale Bedrohungsinformationen in großem Maßstab nutzen und maschinelles Lernen in der Echtzeit-Verhaltensanalyse von Website-Traffic einsetzen, um schädliche Bots zu blockieren und gleichzeitig zu lernen, wie sie in Zukunft noch schneller identifiziert werden können.

Was ihre Handhabung betrifft, sollte sich die ideale Bot-Lösung leicht implementieren und verwalten lassen, ohne dass dafür internes Know-how, kostspielige Wartung oder ständig neue manuelle Anpassungen erforderlich wären. Sie sollte möglichst selten falschen Alarm schlagen und bösartige Bots zielsicher blockieren, dabei echten Nutzern oder hilfreichen Bots aber nicht in die Quere kommen. Kurzum: Sie sollte die Nutzererfahrung aktiv verbessern und optimieren.

Cloudflare Bot Management erfüllt alle diese Anforderungen. Die Lösung setzt Bedrohungsinformationen von mehr als 25 Millionen Websites für die Analyse des Nutzerverhaltens ein, ebenso wie ein Machine Learning-Programm, das mit einer kuratierten Untergruppe von Hunderten Milliarden Anfragen am Tag trainiert wird. Die Erhebung von Fingerprinting-Informationen über Millionen von Webseiten und Applikationen runden den Ansatz ab. Damit kann Cloudflare Unregelmäßigkeiten im Nutzerverkehr proaktiv aufspüren und bei jeder Anfrage zielgenau bewerten, mit welcher Wahrscheinlichkeit sie von einem schädlichen Bot ausgeht. Auf diese Weise können ein ungestörtes Nutzererlebnis gewährleistet und gleichzeitig Bots von der Website ferngehalten werden.

Unter www.cloudflare.com/de-de/ erfahren Sie, wie Sie Ihre Website schützen und ihre Ladezeiten beschleunigen können.

Endnoten

[1] Cloudflare, „Was ist Bot-Traffic?“, Cloudflare Infocenter, letzter Zugriff am 4. März 2020

[2] Cloudflare, 5 BEST PRACTICES: Bescheren Sie Ihrer E-Commerce-Website maximalen Erfolg im Feiertagesgeschäft

[3] Barrett, Brian, „The Likely Reason Disney+ Accounts Are Getting Hacked“,Wired.com, 20. November 2019:gg g -z vz

[4] Alina Bizga, „U.S. retailer J.Crew reveals 2019 security incident to customers“, Security Boulevard.