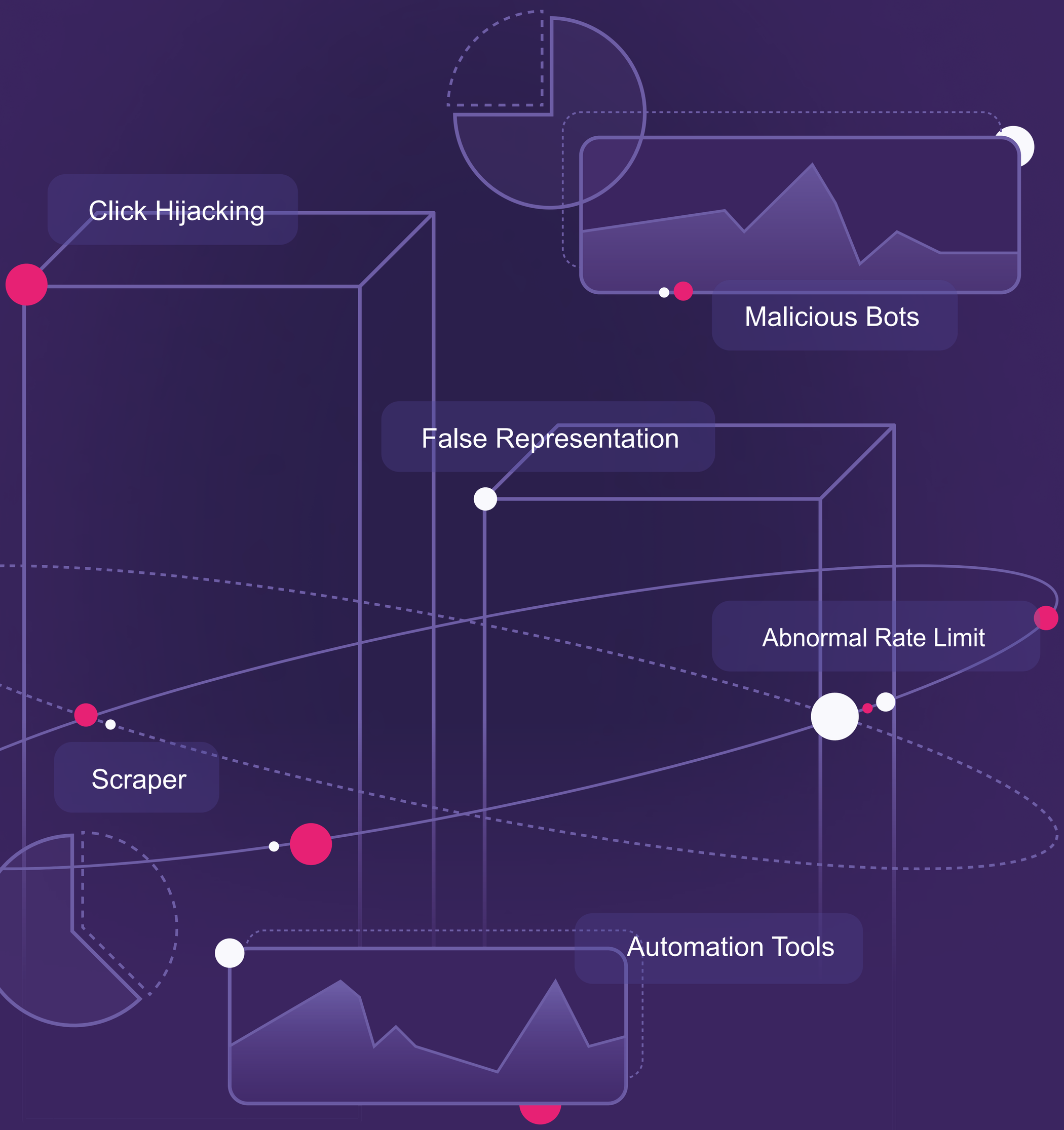
Stand des
Fake Traffic 2024

Wie Bots und Fake User Unternehmen beeinträchtigen und Ineffizienz verursachen.



CHEQ

Inhaltsverzeichnis

Einleitung 3

Überblick & Methodik 4

Fake Traffic Gefahren & Quellen 6

Fake Traffic nach Industrie 7

2023 Fake Traffic Trends: Anstieg in der Urlaubssaison 10

2023 Fake Traffic Trends: Automation Tools 11

2023 Fake Traffic Trends: Advanced Evasion Techniques 12

2023 Fake Traffic Trends: Nutzerumgebungen 13

2023 Fake Traffic Trends: Betriebssysteme 14

2023 Fake Traffic Trends: Browser Details 15

Über CHEQ 16

Einleitung

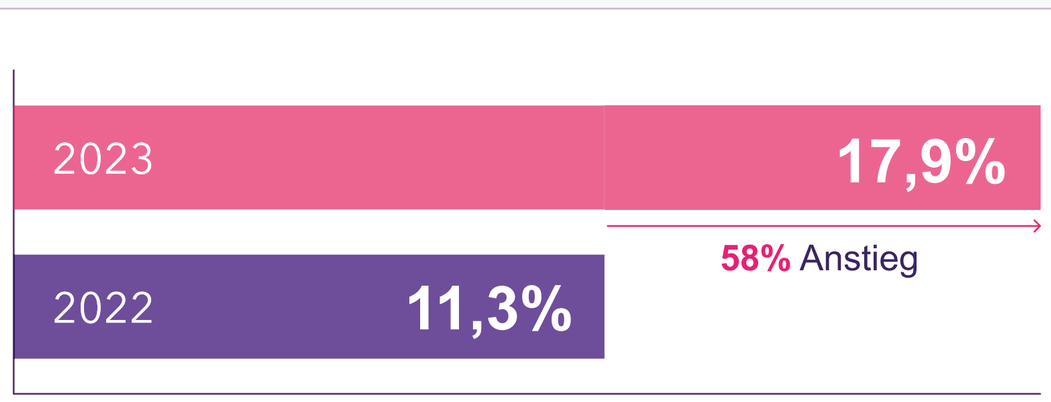
> **Stellen Sie sich eine Welt vor, in der Milliarden unsichtbarer Hände das Internet gestalten, Online-Erlebnisse manipulieren und digitale Ökosysteme stören, während sie sich als echte menschliche Nutzer ausgeben.**

Dies ist keine bloße Phantasieübung, sondern die nackte Realität. 2024 beschränken sich Cyberkriminelle und Betrüger nicht mehr auf einfache Bots und Klick-Farmen, sondern verfügen über hochentwickelte Bots, die menschliches Verhalten imitieren, sich nicht entdecken lassen und ein breites Spektrum an schädlichen Aktivitäten durchführen. Sie scrapen Daten ohne Erlaubnis, vergrößern Engagement-Metriken künstlich, verüben Betrug und bedrohen die Sicherheit und Integrität zahlreicher Websites, mobiler Apps und APIs.

Es ist eine Welt, in der sich sowohl hilfreiche als auch schädliche Automation Tools die Bühne mit zahllosen Nutzern, die keine legitimen Absichten verfolgen, teilen.

Wir nennen dieses Phänomen *Fake Traffic* und das Problem wird immer größer. In unserem zweiten Jahresbericht über den Stand des Fake Traffic hat unsere Analyse des Fake Traffics auf Tausenden von Domains gezeigt, dass 17,9 % des gesamten beobachteten Web-Traffics im Jahr 2023 automatisiert oder fehlerhaft war, was einen Anstieg um 58 % gegenüber 2022 ausmacht, als der Anteil bei 11,3 % lag.

17,9% des gesamten beobachteten Traffics war 2023 fake.



Fake Traffic ist nicht nur ein Ärgernis, sondern ein strategisches Geschäftsproblem. Die Auswirkungen reichen von einer verminderten Werbewirksamkeit und verzerrten Analyseergebnissen bis hin zu größeren Problemen wie Betriebsunterbrechungen, unbefugtem Datenzugriff und der Erosion der Kundenbasis. Zusammen können diese Probleme zu einem Rückgang des Shareholder Values, zu Rufschädigung und sogar zum Verlust von Marktanteilen führen.

Dieses Jahr haben wir unsere Analyse auf ein breiteres Spektrum von Branchen und neue Metriken ausgedehnt, die Bots nach dem von ihnen selbst angegebenen Browser, Betriebssystem und Gerätetyp kategorisieren und so tiefere Einblicke in die Eigenschaften des Fake Traffic erlauben.

Zusätzlich dazu haben wir Automation Tools, die zur Erstellung dieser Bots verwendet werden, wie z. B. Chromedriver und Puppeteer, untersucht. Damit wollten wir ein differenzierteres Verständnis der Technologien, die hinter Fake Traffic stehen, und ihrer Auswirkungen auf digitale Umgebungen gewinnen.

Überblick

Der Überblick über den Stand des Fake Traffic 2024 bietet eine kritische Analyse rasant zunehmender Gefahren in der digitalen Landschaft, einschließlich automatisierter Systeme, Klick-Farmen und Malicious Bots. Der Bericht zeigt die wichtigsten Trends, Instrumente und Auswirkungen auf verschiedene Branchen auf.

2023

ist der Bot Traffic weiter angestiegen

17,9%

des gesamten Web-Traffics war fake

58% YoY

Anstieg von Fake Traffic insgesamt

28% YoY

Anstieg bei allen Bots

Diese Bedrohungen haben sich besonders stark entwickelt

- 32 % YoY Anstieg von **Malicious Bots** Fälle.
- 20% YoY Anstieg entdeckte Bots, die **Automation Tools** wie Selenium und Marionette nutzen.

Schlüsselindustrien waren stark vom Fake Traffic betroffen, darunter

Finanzen & Versicherungen
17,3% Fake Traffic

Einzelhandel & E-Commerce
15,8% Fake Traffic

Software
14,1% Fake Traffic

Bad Actors bevorzugen Desktop User Agents für Angriffe auf Unternehmen.

Betrachtet man den gesamten Fake Traffic, so stammen 71 % vom Desktop und 29 % von mobilen Endgeräten.

71%
Desktop

29%
Mobile Endgeräte

Methodik

CHEQ wertet jeden Besuch aus, indem es in Echtzeit mehr als 2.000 Cybersecurity-Test durchführt, um die Echtheit der User zu validieren.

Die Daten dieses Berichts fußen auf einem Pool von 34 Milliarden Datensätzen, die 2023 von Hunderten von CHEQ-Kunden auf Unternehmensebene betrachtet wurden.

Jeder dieser Datensätze steht für eine einzigartige Interaktion zwischen einer von CHEQ geschützten Kunden-Website, Application oder einer IT- Infrastruktur und einer Reihe von Endgeräten, darunter Smartphones, Tablets, Desktop-Computer, IoT-Devices und Embedded Systems.

Wenn ein Gerät mit einer von CHEQ geschützten Domäne interagierte, wurde es jedes Mal über 2.000 Cybersicherheitsprüfungen in Echtzeit unterzogen, um die Zulässigkeit des Besuchs zu überprüfen.

Jeder als Fake identifizierte Traffic wurde dem Kunden sofort in CHEQ und den integrierten Technologien gemeldet. Der Traffic wurde auf Grundlager umfassender Untersuchungen seiner Attribute eingestuft. Dazu gehörten die Analyse der Traffic-Quellen, sowohl der tatsächlichen als auch der selbst gemeldeten, die Prüfung der verwendeten Gerätetypen, Betriebssysteme und Browser (oder der von den Bots selbst gemeldeten) sowie die Identifizierung der bei der Bot-Erstellung verwendeten Tools und Bibliotheken.

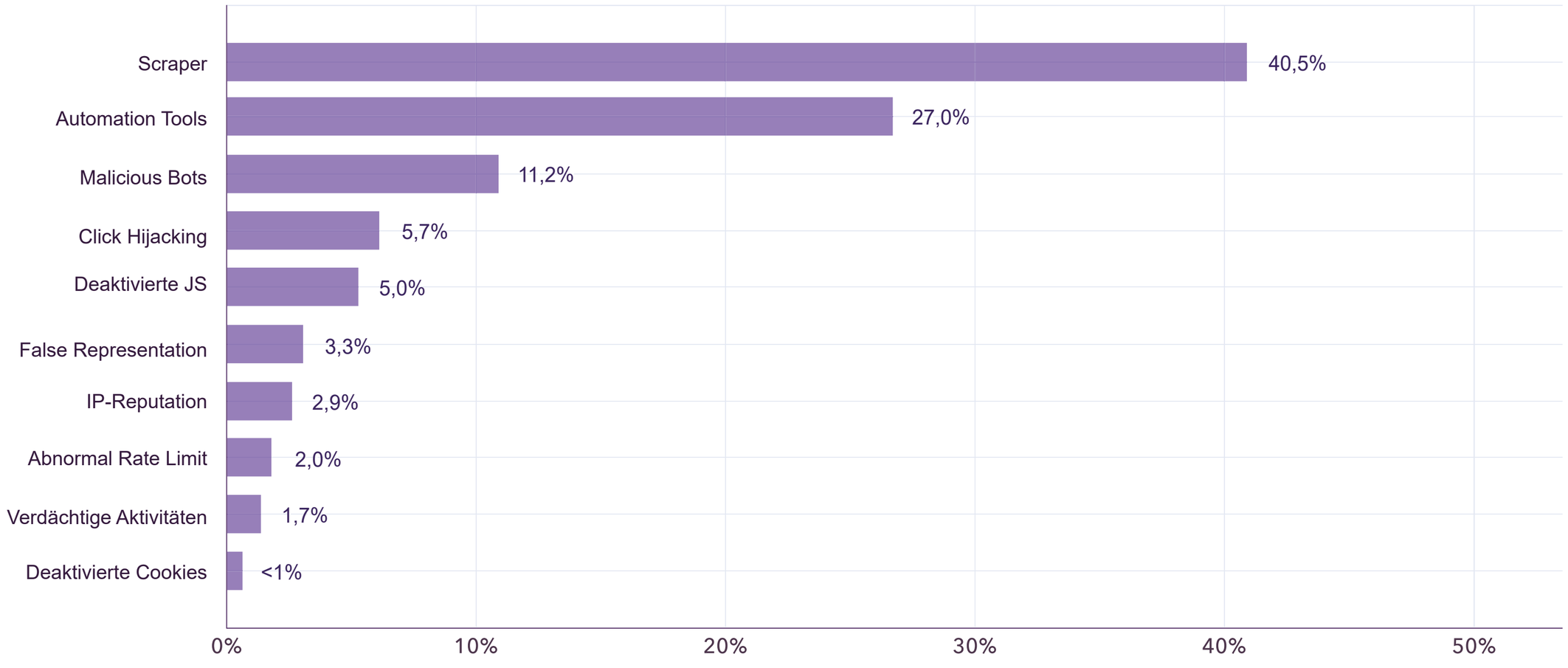
Das übergeordnete Ziel dieser Studie bestand in der Durchführung einer umfassenden Analyse von Fake Traffic in Unternehmen. Dadurch waren wir in der Lage, verwertbare Erkenntnisse und Hinweise zu den Merkmalen, Folgen und Gefahren des Fake Traffics zur Verfügung zu stellen.

Die in diesem Bericht dargestellten Daten wurden einem Standardisierungsprozess unterzogen. Bei diesem wurden die extremsten Ereignisse nicht berücksichtigt, um eine Beeinflussung durch ungewöhnliche oder außergewöhnliche Ereignisse der in diesem Bericht dargestellten Trends auszuschließen.

Fake Traffic Gefahren & Quellen

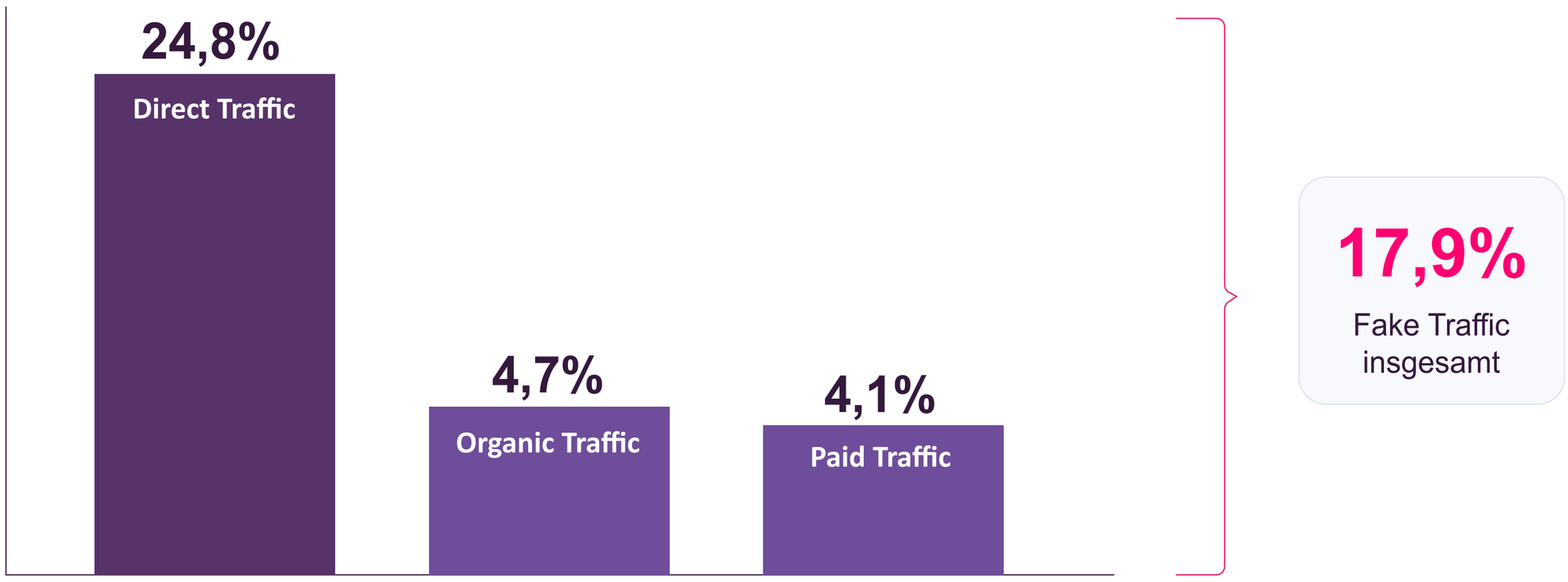
Top 10 der Gefahren

Zu den zehn größten Gefahren in allen Branchen gehörten 2023 Scraper, Automation Tools und Malicious Bots. Dies geschieht parallel zum Anstieg generativer KI, die es den Nutzern leichter macht, Bots zu erstellen.



Quellen des Fake Traffic

Bei der Untersuchung des Ursprungs von Fake Traffic weist Direct Traffic die höchsten Raten auf. 24,8 % ist ein weiterer Anstieg gegenüber den 22,1 % des Vorjahres. Während Direct Traffic manchmal eine große Aufmerksamkeit echter Nutzer zeigen kann, ist es auch für Bots und Bad Actors eine übliche Vorgehensweise, um schnell auf eine Website zuzugreifen, die sie angreifen wollen.



Fake Traffic nach Industrie

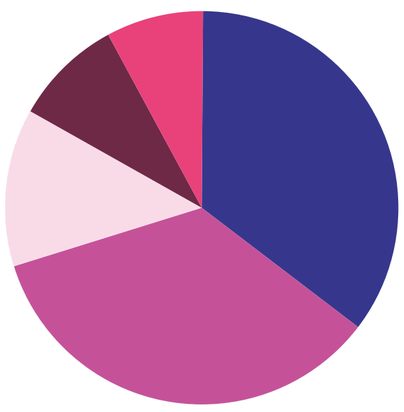
Fake Traffic ist ein weit verbreitetes Problem, das Unternehmen aller Größenordnungen betrifft. Branchen, deren Einnahmen von Online Traffic oder Werbung abhängig sind, sind besonders betrugsanfällig. Unsere Datenanalyse verschiedener Kunden aus unterschiedlichen Bereichen hat ergeben, dass die Unternehmensbranche die Menge des Fake Traffic stark beeinflussen kann.

Schlüsselindustrien wie Einzelhandel und E-Commerce, Software, Finanz- und Versicherungswesen und Hochschulwesen verzeichneten Raten von 15,8%, 14,1%, 17,3% bzw. 15,7%.

Die folgenden Diagramme zeigen die durchschnittliche Fake Traffic Rate für jede Branche, die fünf größten Gefahren und die wichtigsten Quellen des Fake Traffic.

Finanzen & Versicherungen

Finanzdienstleistungen, Banken & Versicherungen



Aufschlüsselung der 5 größten Gefahren:

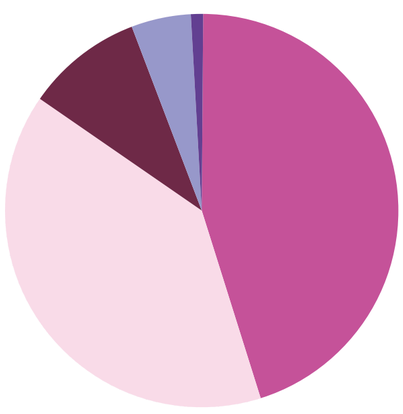
IP-Reputation	35,5%
Automation Tools	35,0%
Scraper	12,2%
Malicious Bots	9,1%
Deaktiverte JS	8,0%

Gesamte Fake Traffic Rate: 17,3%

Direct: 18,9%
Organic: 13,2%
Paid: 10,3%

Gesundheitswesen und Lebenswissenschaften

Medizinische Dienstleistungen, Pharmazeutika und Biotechnologie



Aufschlüsselung der 5 größten Gefahren:

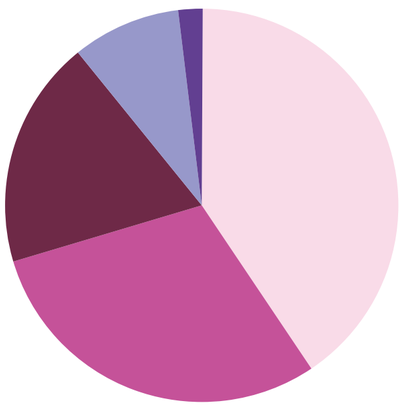
Automation Tools	48,8%
Scraper	39,7%
Malicious Bots	9,0%
False Representation	4,6%
Click Hijacking	1,0%

Fake Traffic Rate: 9,5%

Direct: 17,0%
Organic: 3,4%
Paid: 2,8%

Hochschulwesen

Gemeinnützige und gewinnorientierte Fachhochschulen und Universitäten



Aufschlüsselung der 5 größten Gefahren:

Scraper	41,4%
Automation Tools	29,5%
Malicious Bots	18,7%
False Representation	8,9%
Abnormal Rate Limit	1,3 %

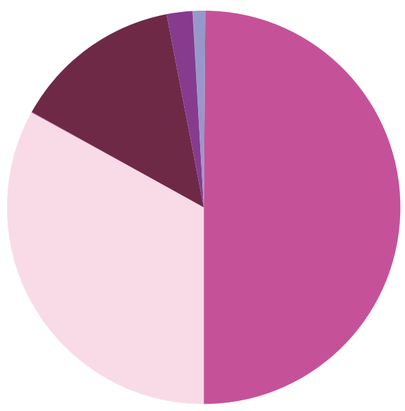
Fake Traffic Rate: 15,7%

Direct: 29,4%
Organic: 4,5%
Paid: 9,0%

Fake Traffic nach Industrie

Produktion

Bauwesen, Innenausbau und Infrastruktur



Aufschlüsselung der 5 größten Gefahren:

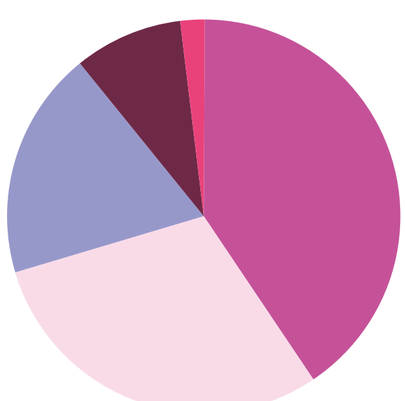
Automation Tools	50,4%
Scraper	33,7%
Malicious Bots	14,0%
Deaktivierte Cookies	<1%
False Representation	<1%

Fake Traffic Rate: 16,8%

Direct: 30,9%
Organic: 3,2%
Paid: 6,0%

Marketing & Advertising

Advertising & Marketing Dienstleistungen & Agenturen



Aufschlüsselung der 5 größten Gefahren:

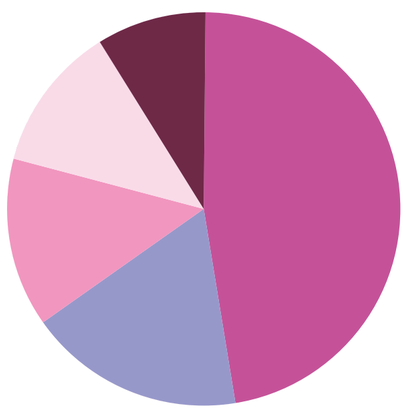
Automation Tools	41,4%
Scraper	29,5%
False Representation	18,7%
Malicious Bots	8,9%
Deaktiviertes JS	1,3%

Fake Traffic Rate: 17,4%

Direct: 29,5%
Organic: 13,6%
Paid: 6,3%

Medien & Verlagswesen

Traditionelle und digitale Zeitungsverlage



Aufschlüsselung der 5 größten Gefahren:

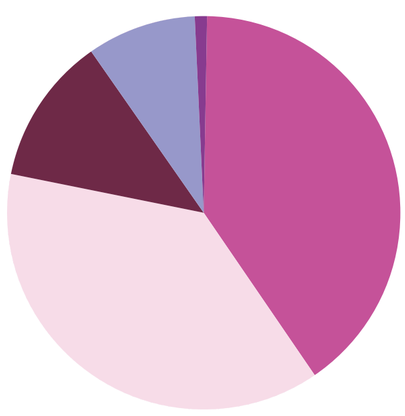
Automation Tools	47,8%
False Representation	17,6%
Verdächtige Aktivitäten	14,2%
Scraper	11,7%
Malicious Bots	8,4%

Fake Traffic Rate: 10,4%

Direct: 10,3%
Organic: 11,8%
Paid: 3,0%

Immobilien

Erschließung, Vermietung & Verkauf von Immobilien



Aufschlüsselung der 5 größten Gefahren:

Automation Tools	47,8%
Scraper	37,8%
Malicious Bots	12,2%
False Representation	9,1%
Deaktivierte Cookies	<1%

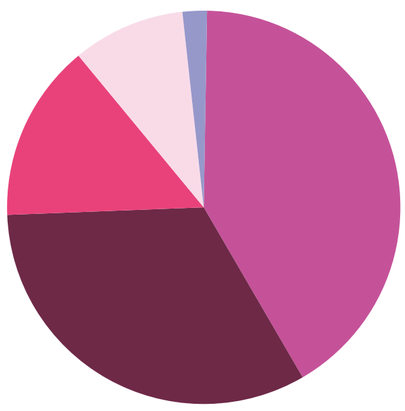
Fake Traffic Rate: 10,6%

Direct: 34,4%
Organic: 3,1%
Paid: 3,4%

Fake Traffic nach Industrie

Einzelhandel & E-Commerce

Traditionelle, Online- & Direktvertriebshändler



Aufschlüsselung der 5 größten Gefahren:

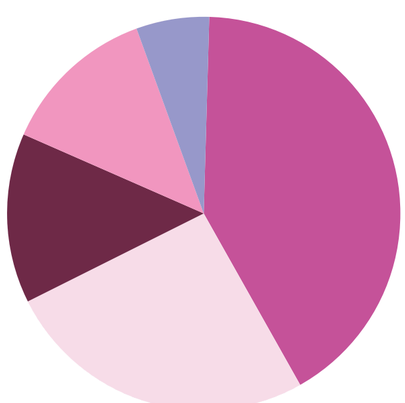
Automation Tools	41,8%
Malicious Bots	32,7%
Deaktiverte JS	14,5%
Scraper	9,0%
False Representation	1,8%

Fake Traffic Rate: 15,8%

Direct: 32,6%
Organic: 3,75%
Paid: 3,3%

Software

Hersteller von Unternehmens- und Verbrauchersoftware



Aufschlüsselung der 5 größten Gefahren:

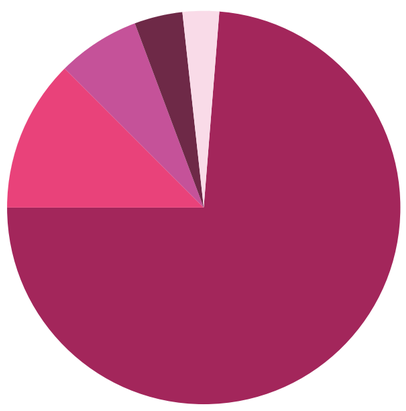
Automation Tools	42,1%
Scraper	25,8%
Malicious Bots	13,5%
Verdächtige Aktivitäten	13,1%
False Representation	5,2%

Fake Traffic Rate: 14,1%

Direct: 22,5%
Organic: 4,5%
Paid: 2,7%

Reisen & Freizeit

Unternehme & Dienstleistungen in den Bereichen Reisen, Gastronomie & Unterhaltung



Aufschlüsselung der 5 größten Gefahren:

Click Hijacking	75,5%
Deaktiverte JS	11,8%
Automation Tools	6,1%
Malicious Bots	3,7%
Scraper	2,7%

Fake Traffic Rate: 11,9%

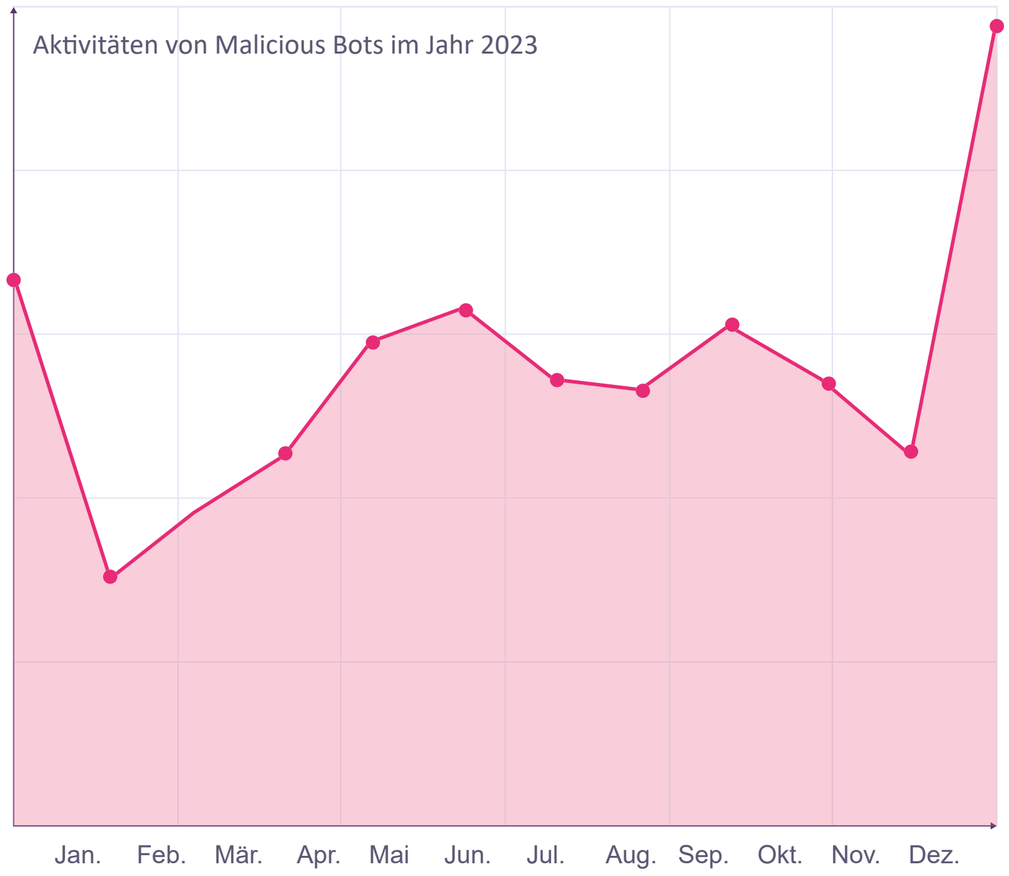
Direct: 13,4%
Organic: 3,1%
Paid: 2,4%

2023 Fake Traffic Trends: Anstieg in der Urlaubssaison

Anstieg schädlicher Aktivitäten in der Urlaubssaison

Im Dezember 2023 gab es einen deutlichen Anstieg des blockierten schädlichen Web-Traffics. Dieser wurde vor allem durch Bots verursacht, die in der Urlaubssaison den Einzelhandel und die Reisebranche zum Ziel hatten.

Dieser Anstieg war durch die Nutzung von Automation Tools gekennzeichnet, deren Ziel es war, Bots als echte Nutzer zu tarnen, insbesondere im Dezember. Die Fähigkeiten dieser Bots stellten eine erhebliche Bedrohung dar, die von Ressourcenverbrauch bis hin zu Denial-of-Inventory-Angriffen reichte.



Fall-Studie: Anstieg von Bots-as-a-Service

Ein weiterer Faktor, der 2023 zum Anstieg schädlichen Web-Traffics beitrug, war die Zunahme von Bots-as-a-Service-Plattformen (BaaS). Diese Plattformen bieten leicht verfügbare, hochentwickelte Automation Tools, die auch von Personen mit minimalen technischen Kenntnissen eingesetzt werden können. Diese zusätzliche Benutzerfreundlichkeit und Verfügbarkeit hat den Aktionsradius potenzieller Angreifer vergrößert und erlaubt es, mit geringem Aufwand weitreichende Angriffe zu inszenieren.

Ein erwähnenswerter Fall war ein gezielter Angriff auf eine Domain der Reisebranche, der im Dezember stattfand. Wir entdeckten eine bekannte BaaS-Plattform, die einen 14-fachen Anstieg bei versuchten betrügerischen Klicks durch Google Search Ads verzeichnete. Dies war offensichtlich ein gezielter Versuch, das PPC-Budget des Zielunternehmens während einer kritischen Verkaufsperiode zu erschöpfen.

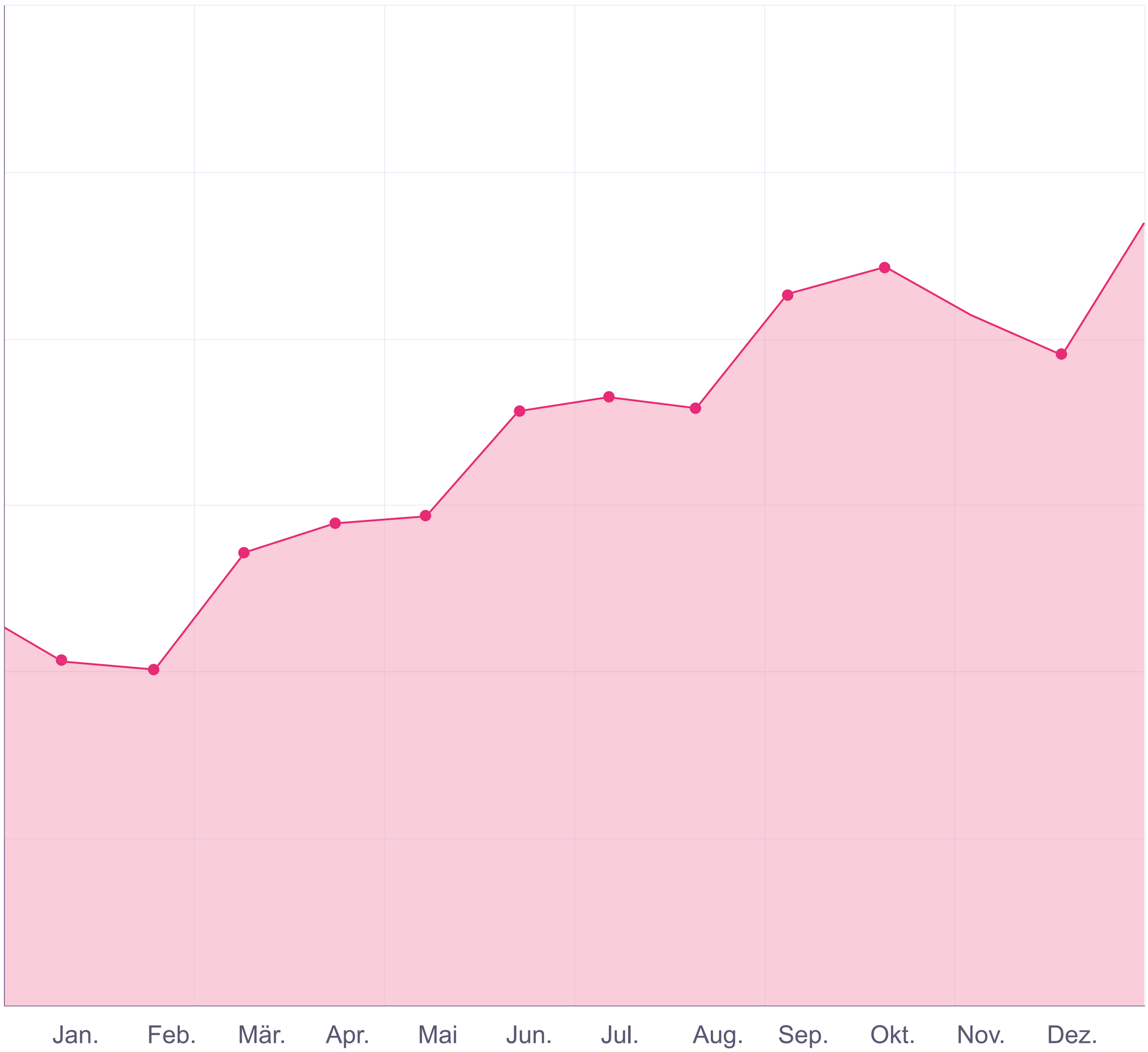
2023 Fake Traffic Trends: Automation Tools

Einfache Browser-Automation Tools machten 2023 24% des ganzen Fake-Traffics aus

2023 machten einfache Browser-Automation Tools 24,0% des ganzen Fake-Traffics aus. Der Einzelhandel und der E-Commerce waren, gemessen am Volumen, am stärksten betroffen, was auf eine starke Verbreitung der Nutzung dieser Tools für Scraping und Missbrauch hindeutet.

Die am häufigsten entdeckten Automation Tools waren Selenium, ein beliebtes Open-Source-Framework zur Browser-Automatisierung, und Marionette, Mozillas Automatisierungstreiber zur Steuerung und Interaktion mit dem Firefox-Webbrowser.

Aktivitäten von Automation Tools 2023



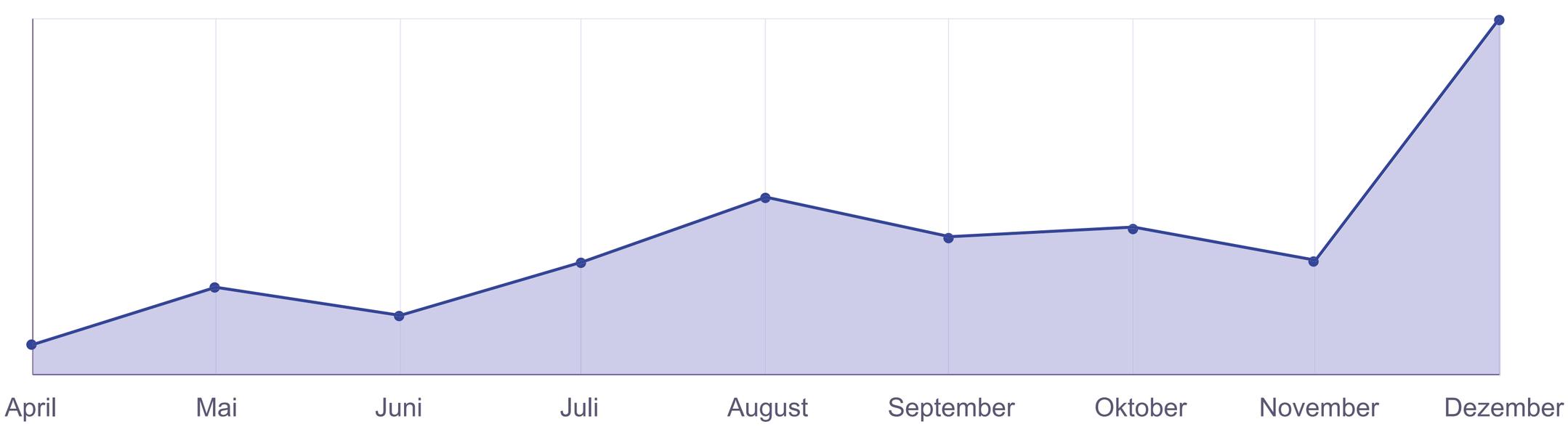
2023 Fake Traffic Trends: Advanced Evasion Techniques

Tracking der zunehmenden Nutzung von unbekannten ChromeDriver und Puppeteer-extra-plugin-stealth

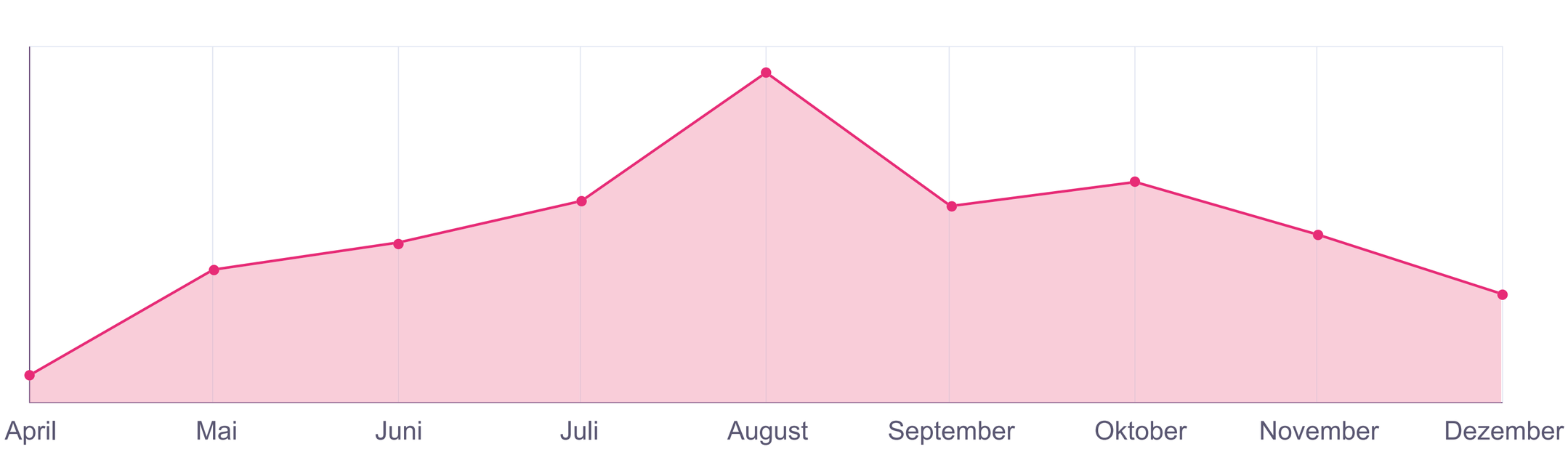
Headless Chrome ist sowohl für Developer, die automatisierte Tests durchführen, als auch für Bot-Entwickler, die schädlichen Web-Traffic automatisieren, ein Segen. Jedoch ist seine Verwendung in der Automatisierung leicht durch Fingerprinting und durch bestimmte Eigenschaften wie "navigator. webdriver" zu entdecken. Um dem zu entgehen, nutzen Bot-Hersteller hochentwickelte Tools wie unbekannte ChromeDriver und dem Puppeteer-extra-stealth-plugin ,die Automatisierungssignale maskieren und menschliche Interaktionen besser imitieren sollen. Diese Tools modifizieren Browser-Attribute, die von Anti-Bot-Systemen überprüft wurden, und lassen so automatisierte Browser als normale Benutzer-Browser erscheinen.

Unsere Daten belegen eine steigende Verbreitung und die potenziellen Auswirkungen dieser Betrugsmethoden. Im zweiten bis vierten Quartal 2023 stieg die Nutzung von unentdeckten ChromeDrivern sprunghaft an, wobei entdeckte Fälle 2023 um 650 % zunahmen. Ähnlich stiegen die Einsätze von Puppeteer-extra-plugin-stealth, dem gängigeren der beiden Tools, bei der Höchstauslastung um 414 % an.

Bot mit unerkanntem ChromeDriver, Q2-Q4, 2023



Puppeteer-extra-plugin-stealth, Q2-Q4, 2023



2023 Fake Traffic Trends: Benutzerumgebung

Fake Traffic nach Benutzerumgebung

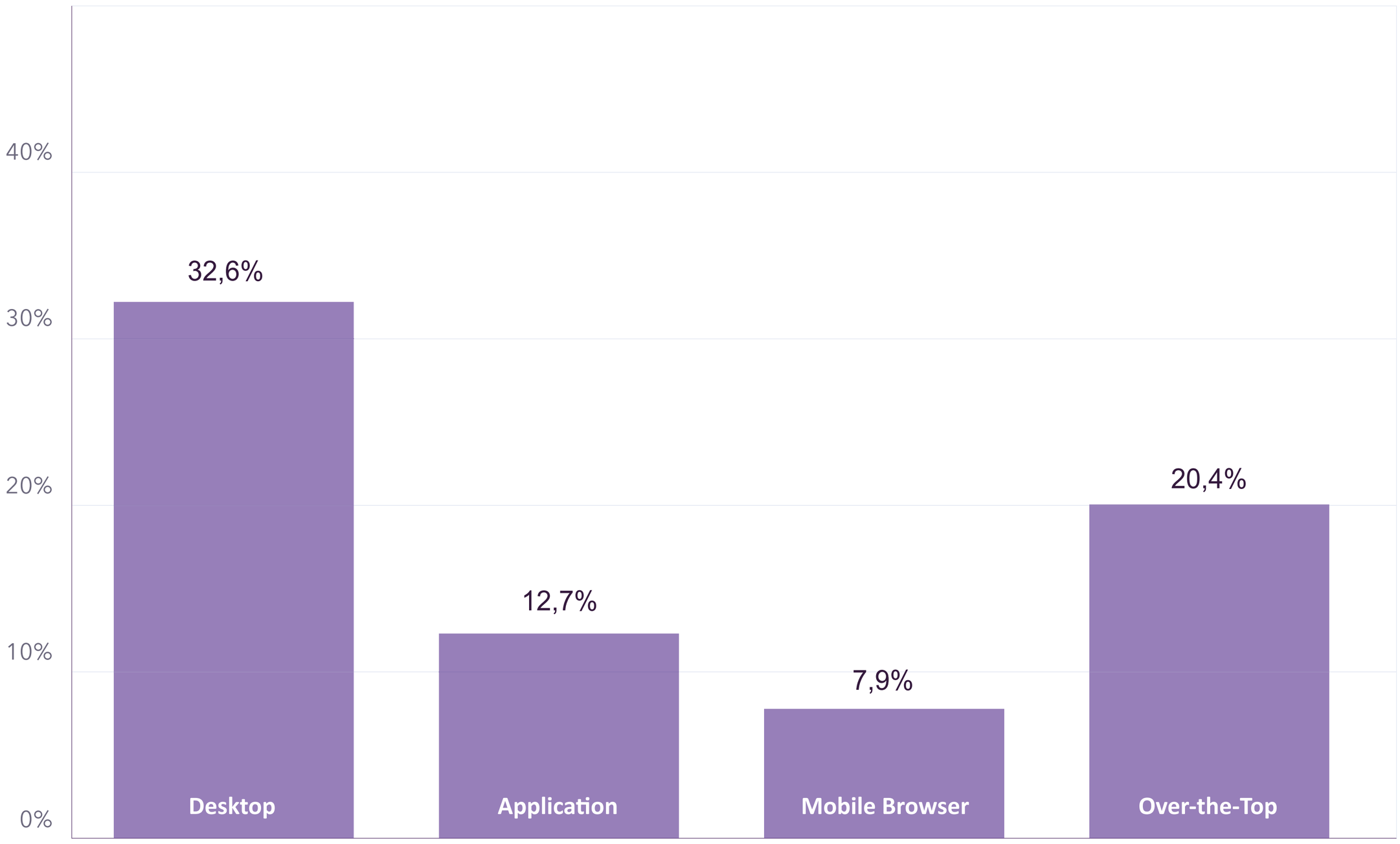
Die Analyse des Fake Traffic nach der (angeblichen) Benutzerumgebungskategorie macht deutliche Unterschiede sichtbar. Desktop-Plattformen weisen eine hohe Fehlerquote von 32,6 % auf. Das bedeutet, dass sich Angreifer weiterhin auf diese traditionellen Computerumgebungen konzentrieren, da diese vertraut sind und auch in Unternehmen und Betrieben häufig verwendet werden.

Die auffällig hohe Fake-Traffic-Rate von 20,4 % für Over-the-Top (OTT)-Umgebungen – Technologien, die Streaming-Inhalte über internetfähige Geräte bereitstellen – ist sowohl auf die relativ hohen Kosten zurückzuführen, die mit OTT-Werbung zusammenhängen (im Durchschnitt 25 bis 40 US-Dollar CPM), als auch auf die Art der OTT-Ads Auslieferung.

Serverseitige Anzeigeneinfügung (SSAI) ermöglicht es Werbetreibenden, Anzeigen nahtlos in Inhalte einzufügen. Dies kann aber auch unbeabsichtigt die Tür für Anzeigenbetrug öffnen, indem clientseitige Ad Verification Tools daran gehindert werden, die Legitimität von Anzeigen zu überprüfen, Nutzerdaten zu maskieren und Ad-Stacking und Domain-Spoofing zu ermöglichen.

Im Gegensatz dazu zeigt das mobile Web mit 7,9 % eine deutlich niedrigere Fake Traffic Rate. Dies liegt am geringeren Fokus der Angreifer darauf, da die Erträge im Vergleich zu Desktop- oder OTT-Plattformen vermeintlich niedriger angesetzt werden.

Fake Traffic nach Umgebung



2023 Fake Traffic Trends: Betriebssysteme

Fake Traffic nach Betriebssystemen

Unsere Analyse zeigt überraschende Einblicke in die Verbreitung von Fake Traffic über verschiedene Endgeräte 2023 und beleuchtet entstehende Trends unter Bad Actors.

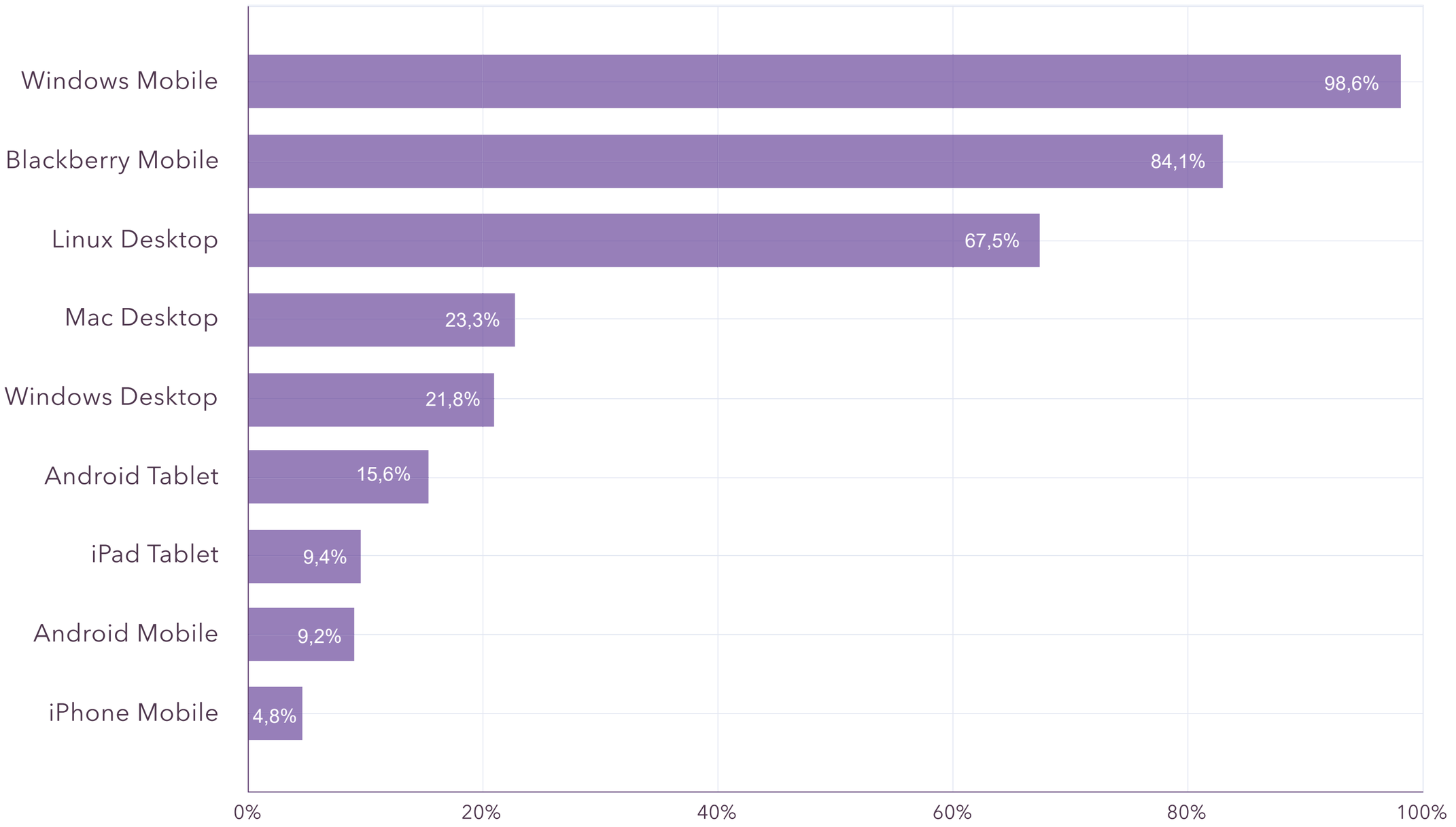
Ein interessantes Phänomen ist folgendes: Die relativ geringe Menge an Web-Traffic, die von nicht mehr existierenden mobilen Plattformen – Windows Mobile und Blackberry – beobachtet wurde, wies bei weitem die höchsten Fake Traffic Rates von allen mobilen Betriebssystemen auf.

Das hängt wahrscheinlich eher mit veralteten Bots zusammen, die wohl seit Jahren nicht mehr geupdatet wurden, als mit Cyberkriminellen, die die Recycling-Tonnen für ihre Klick-Farmen plündern. Es besteht auch eine geringe Wahrscheinlichkeit, dass sich Angreifer (erfolglos) als Nischenplattformen tarnen, um nicht bemerkt zu werden.

Diese Ergebnisse betonen die Signifikanz einer gründlichen Untersuchung von Traffic-Quellen und einer Implementierung robuster Überprüfungsmechanismen, um die Auswirkungen betrügerischer Aktivitäten zu verringern.

Zudem zeigt die höhere Fake Traffic Rate auf bekannten Desktop-Geräten im Vergleich zu bekannten mobilen Gegenstücken, wie attraktiv Desktop-Plattformen für Betrüger sind. Die große Leichtigkeit, mit der Bot-Angriffe auf Desktops durchführbar sind, ist eine enorme Herausforderung für Marketer, da diese betrügerischen Praktiken die Leistungsmetriken verzerren und das Vertrauen in digitale Werbekanäle untergraben.

Betriebssysteme nach Fake Traffics Rate



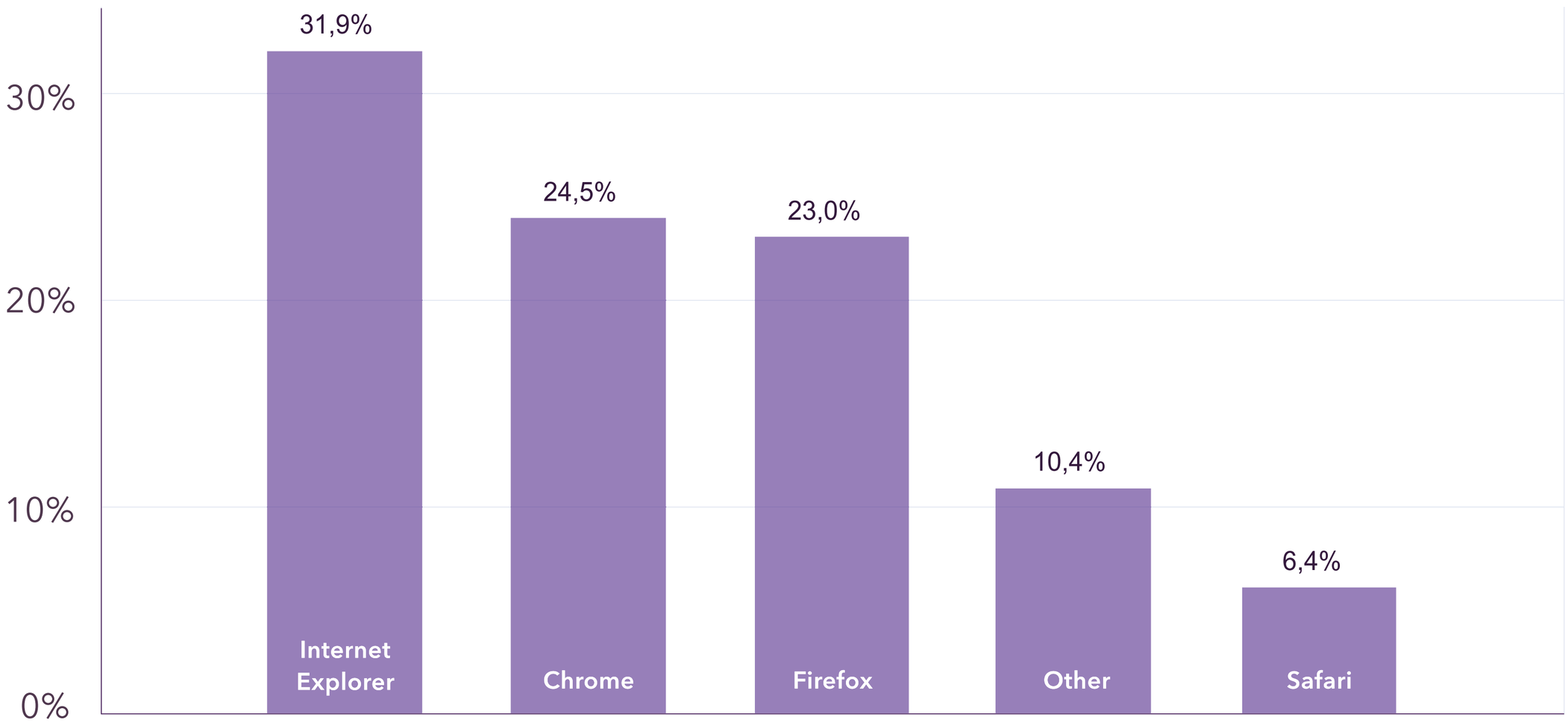
2023 Fake Traffic Trends: Browser Details

Fake Traffic nach Browser

Die Untersuchung von Browser-Informationen, die aus User Agents gewonnen werden, bietet zusätzliche Einblicke in die Dynamik von Fake Traffic. Es unterstreicht die Notwendigkeit von Fake Traffic, sich anzupassen und unauffällig zu wirken.

Der Internet Explorer (IE) hatte trotz seiner geringeren Nutzerbasis eine höhere Fake Traffic Rate von 31,9 %. Dies beweist das Vorhandensein eines Markts für ältere oder seltener aktualisierte Browser unter Bad Actors, die nach einer Plattform suchen, die anfälliger für Ausbeutung ist.

Browser nach Fake Traffic in Prozent



Zusammenfassung

Die Bedrohung durch Bots und Fake Traffic ist nach wie vor dynamisch und allgegenwärtig. Sie erfordert proaktive und anpassungsfähige Maßnahmen von Unternehmen in allen Branchen.

Da 2023 das Jahr des Durchbruchs für die Einführung generativer KI war, führte dies dazu, dass hier eine neue Dimension in diesem Bereich berücksichtigt werden muss. Generative KI-Technologie hat das Potenzial, die Erstellung von Bots zu vereinfachen, Fehlinformationen extrem schnell zu verbreiten und Unternehmen durch Scraping für Sprachlernmodelle potenziellen Urheberrechtsverletzungen preiszugeben. Diese Verfügbarkeit könnte zu einem Anstieg neuer Bots führen, die digitale Plattformen überschwemmen und die Risiken im Zusammenhang mit Fake Traffic und automatisierten Angriffen erhöhen.

Durch dauerhafte Achtsamkeit und kontinuierliche Verbesserung der Abwehrmaßnahmen können Unternehmen die Risiken mindern, die mit Bots und Fake Traffic im Zusammenhang stehen und so ihr Kapital, ihren Ruf und ihr Gewinnpotential in der sich ständig verändernden Cyberlandschaft schützen. Proaktive Maßnahmen, die den Wandel in der KI-Technologie berücksichtigen, sind entscheidend, um einen Vorsprung gegenüber neuen Bedrohungen zu haben und eine sichere digitale Präsenz zu garantieren.

Über *CHEQ*

CHEQ Marktführer im Bereich Go-to-Market Security. Mehr als 15.000 Unternehmen, von aufsteigenden Marken bis hin zu den Fortune 50, vertrauen CHEQ und schützen geschäftskritische digitale Interaktionen vor schädlichen, automatisierten und von Menschen inszenierten Bedrohungen.

Mit seiner unvergleichlichen, kontextspezifischen Detection Engine bietet CHEQ das umfangreichste Set an Lösungen zur Sicherung von Go-to-Market-Aktivitäten. CHEQ bietet Schutz vor Bedrohungen der Geschäftskontinuität, der Markenreputation, der Einhaltung von Datenschutzbestimmungen und der Marketingeffektivität. Das ist der Grund, warum CISOs CHEQ vertrauen, Marketer CHEQ lieben und sich immer mehr Unternehmen für CHEQ entscheiden.

Erfahren Sie, wie Bots und User mit böswilligen Absichten Ihre Go-to-Market-Bemühungen schädigen.
Fordern Sie noch heute einen kostenlosen Website-Scann an.

Unsere Kunden lieben Uns auf G2

Führer
2024

Am einfachsten ins Geschäft zu kommen mit
2024

Bester Kundendienst
2024

Impulsgeber
2024