imperva
a Thales company

#2025BADBOTREPORT

2025

BAD BOT REPORT

The Rapid Rise of Bots and the Unseen Risk for Business

Executive Summary

The Role of AI in Bot Attacks

The rise in the number of accessible AI tools has significantly lowered the barrier for entry for cyber attackers enabling them to create and deploy malicious bots at scale. With generative AI simplifying bot development, automated threats are evolving rapidly - becoming more sophisticated, evasive, and widespread, fueling the growth of both simple and advanced bad bots. Attackers now use AI not only to generate bots but also to analyze failed attempts and refine their techniques to bypass detection with greater efficiency.

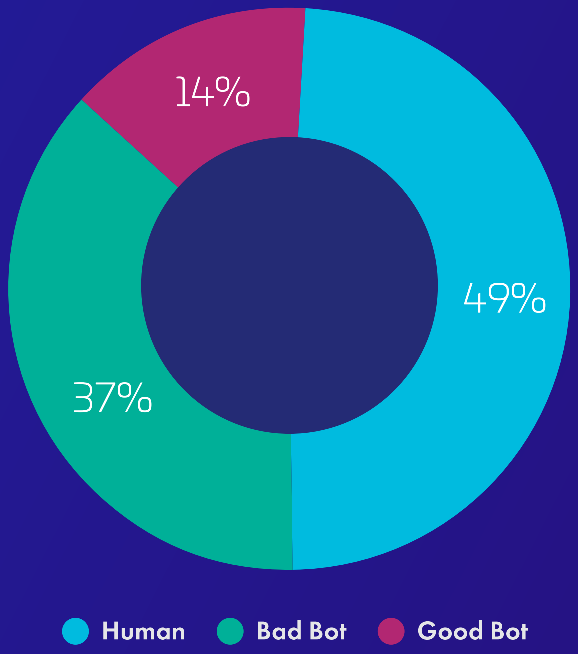
The resulting emergence of more sophisticated, evasive bad bots puts businesses at greater risk than ever before. As automated traffic volumes increase, security teams must adapt their approach to application security, facing increasing pressure to counter an evolving threat landscape in which bots are gaining the upper hand.

Automated Traffic Surpasses Human Traffic

For the first time in a decade, automated traffic surpassed human activity, accounting for 51% of all web traffic in 2024. This was largely driven by the rapid adoption of AI and large language models (LLMs), which have made bot creation more accessible and scalable.

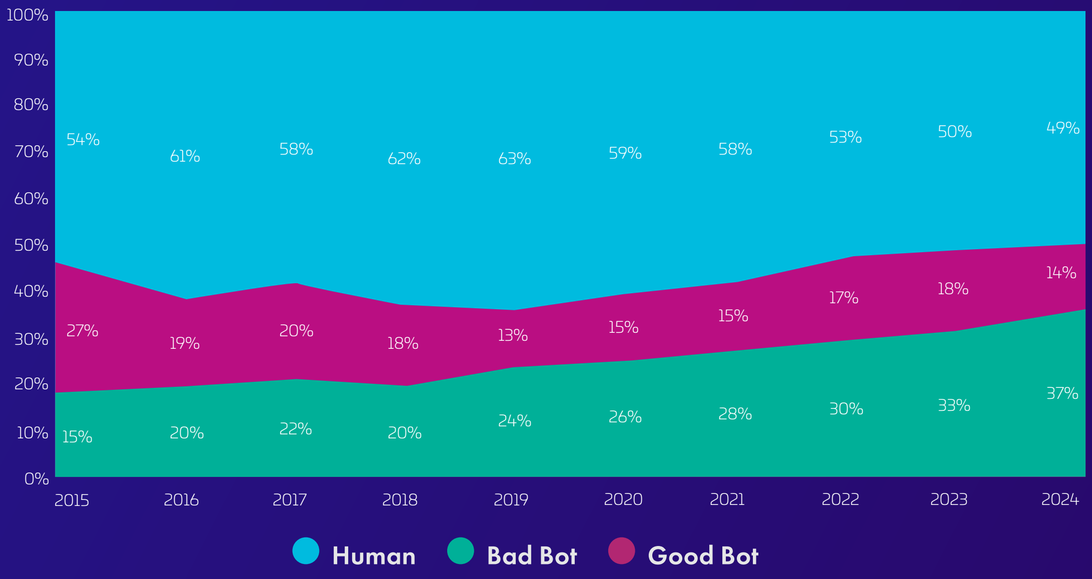
At the same time, bad bot activity has risen for the sixth consecutive year, with malicious bots now making up 37% of all internet traffic, a sharp increase from 32% in 2023.

GLOBAL INTERNET TRAFFIC PROFILE IN 2024



The chart below illustrates the steady rise of bad bots as a percentage of total web bot traffic over the years. In 2015, bad bots accounted for just 19% of all bot traffic. Growth spiked in 2019, largely influenced by unprecedented online usage during the COVID-19 pandemic, a trend that has continued, with bad bot traffic reaching 37% in 2024.

GLOBAL INTERNET TRAFFIC FOR THE PAST 10 YEARS



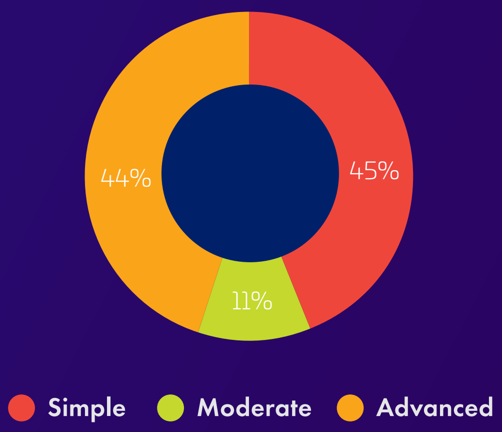
The sharp rise in bot traffic is alarming, and with the emergence of AI raises questions about how we can stem the flow of bot traffic to protect businesses and maintain fair markets.

Bot Attack Sophistication Trends

In 2024, advanced and moderate bot attacks accounted for 55% of all bot attacks. Attackers increasingly employ sophisticated techniques to emulate human traffic and carry out malicious activities, making these attacks harder to detect and mitigate.

However, there has been a significant shift in the dynamics of bot attack sophistication. Simple, high-volume bot attacks have grown substantially, now comprising 45% of all bot attacks—up from 40% in 2023. This rise can be attributed to the increasing accessibility of AI-powered automation tools, which allow attackers with less technical expertise to launch bot attacks easily.

BOT SOPHISTICATION IN 2024



OWASP Automated Threats Account for Almost a Third of All Attacks

In the past year, 31% of all attacks recorded and mitigated by Imperva were automated threats, as defined by the OWASP. The OWASP 21 Automated Threats are a set of automated cyberattacks that leverage bots and scripts to exploit web application vulnerabilities at scale, bypass security controls, and disrupt businesses across various industries, and represent some of the most common and critical vulnerabilities facing web applications. Their widespread nature and the ease with which attackers exploit them make them a primary concern for any organization's security strategy.

A deeper look into the attack types reveals that 25% of mitigated attacks were sophisticated bad bots specifically targeting and abusing business logic.

Why Modern APIs Must Defend Against Bad Bots

In 2024, the Imperva Threat Research team observed a significant surge in API-directed attacks, with 44% of advanced bot traffic targeting APIs. This report includes a section dedicated to API Security, which looks into how bad bots targeting API business logic are a major threat to businesses and how protecting APIs is not just a security measure but safeguarding the foundation of your digital ecosystems.

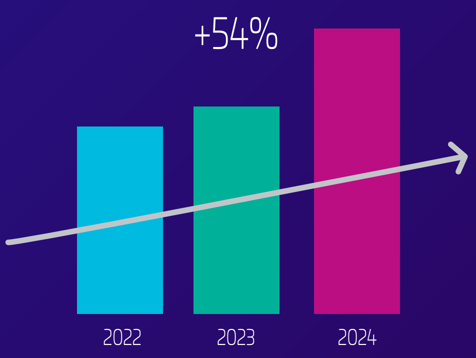
Residential Proxies Remain a Preferred Evasion Tactic

By leveraging residential proxies, bad bots can mimic legitimate traffic from a residential address, making detection more challenging. In fact, 21% of all bot attacks using internet service providers (ISPs), were conducted through residential proxies - a key evasive tactic commonly employed by advanced attackers.

Account Takeover Attacks

The number of Account Takeover (ATO) attacks has increased significantly, rising by 40% since last year and by 54% since 2022. This surge is likely driven by cybercriminals using AI and machine learning to automate credential stuffing and brute-force attacks, making them more sophisticated and harder to detect.

GROWTH OF ATO ATTACKS 2022 TO 2024



> **“25% of mitigated attacks were sophisticated bad bots specifically targeting and abusing business logic.”**

Contents

Key Findings

51% AMOUNT OF AUTOMATED INTERNET TRAFFIC

AMOUNT OF INTERNET TRAFFIC MADE UP OF BAD BOTS 37%

14% AMOUNT OF INTERNET TRAFFIC MADE UP OF GOOD BOTS

55%

PROPORTION OF ADVANCED OR MODERATE BOT ATTACKS IN 2024

45%

PROPORTION OF SIMPLE BOT ATTACKS IN 2024

44%

PERCENTAGE OF ADVANCED BOT ATTACKS TARGETING APIS

55%

SURGE IN API DATA LEAKAGE & API VIOLATIONS IN 2024

25%

PERCENTAGE OF BOT ATTACKS TARGETING BUSINESS

19%

PERCENTAGE OF ACCOUNT TAKEOVER ATTACKS TARGETING APIS

46%

PERCENTAGE OF BOT ATTACKS USING CHROME TO APPEAR AS LEGITIMATE TRAFFIC

14%

PERCENTAGE OF ALL LOGINS THAT WERE ACCOUNT TAKEOVER ATTEMPTS

31%

PERCENTAGE OF ATTACKS THAT WERE OWASP AUTOMATED THREATS

2 MILLION

DAILY AVERAGE NUMBER OF AI-ENABLED ATTACKS

27%

PERCENTAGE OF BOT ATTACKS TARGETING THE TRAVEL INDUSTRY IN 2024

13 TRILLION

NUMBER OF BOT REQUESTS BLOCKED BY IMPERVA IN 2024

40%

PERCENTAGE GROWTH OF ACCOUNT TAKEOVER ATTACKS IN 2024

Bot Attacks Exploit API Business Logic

Businesses are increasingly relying on APIs, driven by the rapid expansion of digital transformation, AI-powered automation, and the growing demand for seamless integration across platforms. APIs are the backbone of modern applications, enabling businesses to connect services, streamline operations, and deliver personalized customer experiences at scale. They power everything from payment processing and supply chain management to AI-driven analytics and third-party integrations, making them essential for agility, innovation, and competitive advantage. As organizations continue to adopt cloud-based services and microservices architectures, APIs provide the critical infrastructure needed to enhance efficiency, accelerate product development, and unlock new revenue streams.

The power behind each API is its business logic —the rules and processes that dictate how it functions interacts with data and facilitates critical business operations. APIs enable automation, real-time decision-making, and seamless integrations, making them indispensable to modern businesses. However, their very functionality also makes them a prime target for bad bots, which manipulate API logic to commit fraud, scrape data, and bypass security controls.

Bad bots are no longer just overwhelming API endpoints—they are evolving to exploit the business logic that underpins these systems. Attackers deploy bots to target vulnerabilities in API workflows, automating payment fraud, account hijacking, and data exfiltration. Because API business logic is unique to each organization, traditional security measures relying on known attack signatures often fail. This allows bots to mimic legitimate user behavior and evade detection. Attackers aren't merely testing vulnerabilities—they're automating large-scale fraud that drains revenue, erodes customer trust, and imposes steep financial losses, regulatory penalties, and reputational damage.

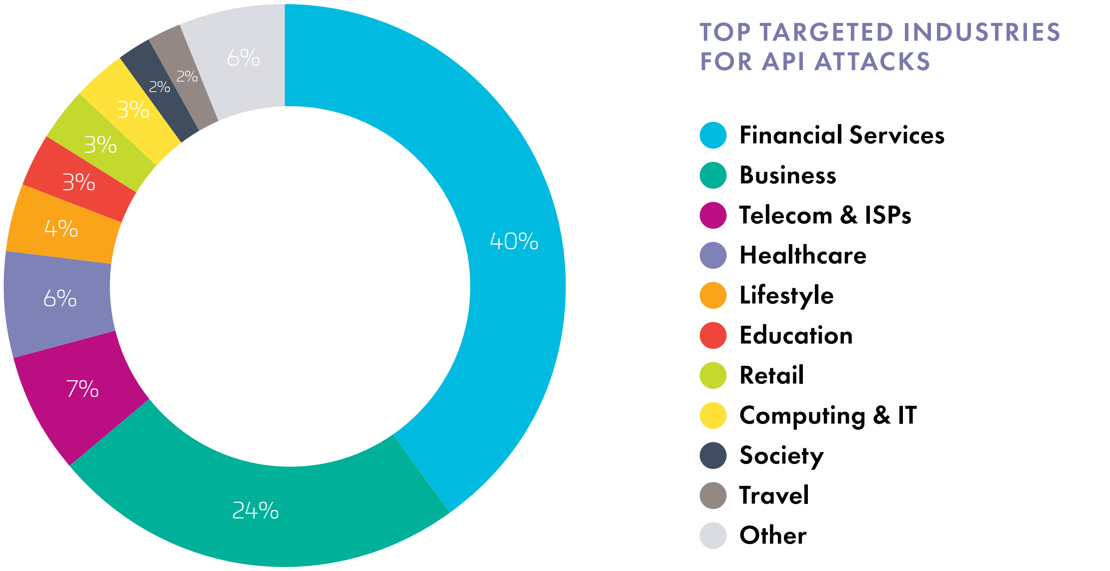
The following analysis from the Imperva Threat Research team highlights how bad bots target APIs, the top industries at risk, the techniques and tactics used, and emerging attack vectors shaping the threat landscape.

API vs. Web Applications

In 2024, the Imperva Threat Research team observed a significant surge in API-directed attacks, with 44% of advanced bot traffic targeting APIs—compared to just 10% targeting web applications. This highlights a deliberate shift by attackers toward API endpoints that handle sensitive and high-value data.

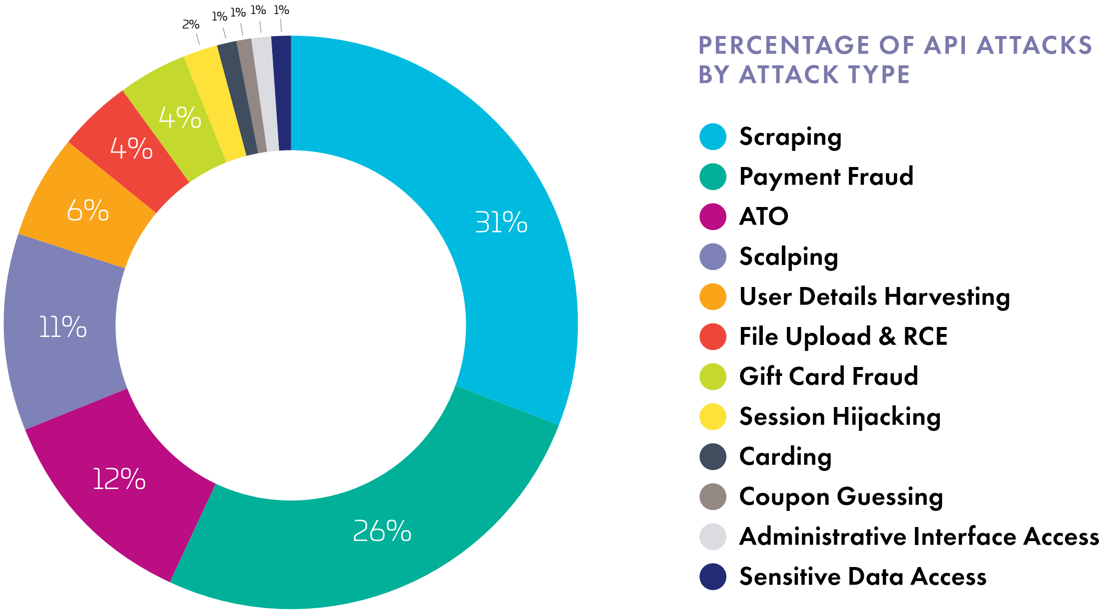
Top Targeted Industries for Bot Attacks on APIs

Financial services, telecom, healthcare and retail are among the top ten most targeted industries for bot attacks on APIs. These sectors depend on APIs for critical operations and sensitive transactions, making them prime targets for sophisticated bot attacks.


TOP TARGETED INDUSTRIES FOR API ATTACKS

API Attack Techniques & Tactics

Our analysis of 2024 API bot attacks reveal a multifaceted threat landscape, where adversaries employ a range of tactics to exploit API vulnerabilities:


PERCENTAGE OF API ATTACKS BY ATTACK TYPE

Data Scraping

~31% of API Attacks

Bots extract vast amounts of data by exploiting APIs that expose sensitive or proprietary information. This method is favored because it enables attackers to automate the collection of valuable datasets, such as user details, product information, and internal metrics, with minimal resistance. The high volume of data scraping not only facilitates further criminal activities but could also provide competitive intelligence.

Payment Fraud

~26% of API Attacks

Targeting financial transaction endpoints, attackers manipulate payment processes to commit fraud. Representing roughly 26% of attacks, this technique involves exploiting vulnerabilities in checkout systems to trigger unauthorized transactions or abuse promotional mechanisms. The immediate financial impact, combined with the erosion of customer trust, makes payment fraud a highly attractive target for bad bots.

Account Takeover

~12% of API Attacks

Comprising around 12% of the attack landscape, account takeover attacks (ATO) leverage stolen or brute-forced credentials to gain unauthorized access to user accounts. Once in control, attackers can access sensitive personal and transactional data, often leading to broader security breaches and further exploitation.

Scalping

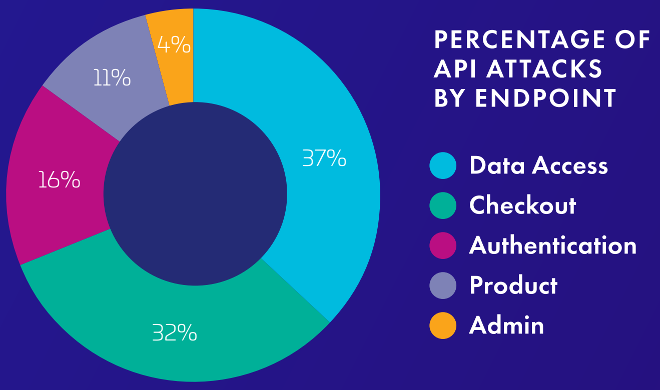
~11% of API Attacks

Scalping attacks, accounting for approximately 11%, involve bots rapidly purchasing or reserving large volumes of high-demand items or services. This tactic not only disrupts fair consumer access but also undermines market dynamics by allowing attackers to resell these items at inflated prices.

In addition to these primary techniques, our report also highlights other methods such as Gift-Card Fraud (~4), Remote Code Execution (~4%), and Session Hijacking (~2%). The common denominator across all these tactics is the exploitation of inherent API vulnerabilities, ranging from misconfigurations and insufficient rate limiting to weak authentication protocols.

Endpoint-Specific Bot Attacks

The chart below indicates that bad bots strategically target API endpoints that handle high-value and sensitive operations. Here's a detailed analysis of the observed trends and the probable reasons behind these attack vectors:



Data Access Endpoints

~37% of API Attacks

These endpoints are responsible for retrieving sensitive or proprietary information, making them a goldmine for attackers. The high attack rate of approximately 37% suggests that adversaries are heavily invested in scraping and exfiltrating data. Such data can fuel further criminal activities or serve as competitive intelligence. The attractiveness of data access endpoints stems from the sheer volume and sensitivity of the information they control, often with less stringent security measures compared to transactional endpoints. To counter this, security professionals should enhance monitoring, enforce strict access controls, and deploy anomaly detection systems to flag unusual data retrieval patterns.

Checkout Endpoints

~32% of API Attacks

Critical for processing financial transactions, checkout endpoints face around 32% of all API attacks. These endpoints are a prime target because any disruption here directly impacts revenue and customer trust. Attackers exploit vulnerabilities to manipulate payment processes, commit fraud, or abuse business logic, leading to unauthorized financial activities. The significant focus on checkout processes underscores the need for robust transaction security, including real-time monitoring, layered authentication, and proactive fraud detection measures.

Authentication Endpoints

~16% of API Attacks

Authentication endpoints, which facilitate identity verification and access control, account for 16% of API bot attacks. These endpoints are targeted to bypass multi-factor authentication, abuse token-based authentication, and manipulate session handling. Given that they serve as the first line of defense in securing user access, any compromise here can lead to account takeovers and broader breaches. Strengthening these endpoints with robust, dynamic authentication protocols and regular audits is crucial to mitigate the risk of unauthorized access.

Overall, the focus on data access, checkout, and authentication endpoints reflects a calculated strategy by attackers to exploit the most critical and vulnerable areas of API infrastructure.

New Exploitation Methods

Beyond traditional tactics, bad bots are now exploiting API vulnerabilities via misconfigured third-party integrations and parameter tampering. These emerging methods enable attackers to bypass established security measures more effectively.

The Emergence of AI-Powered Attacks

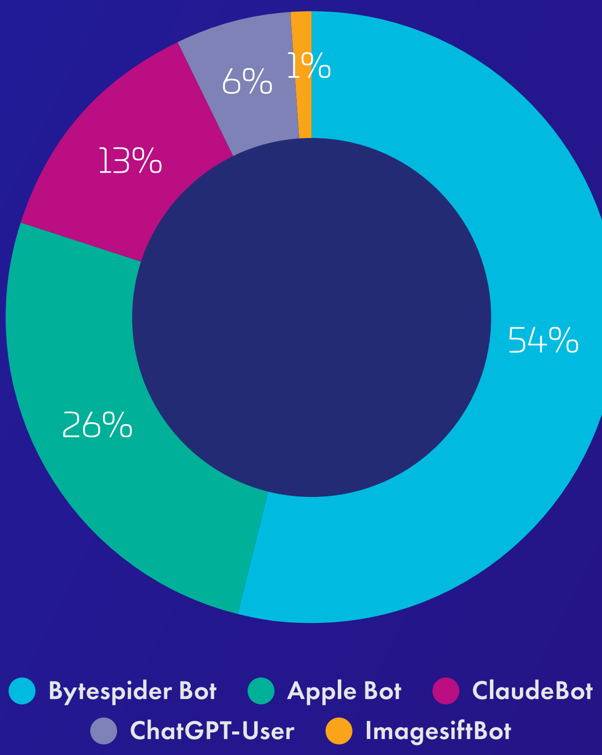
In 2024, we witnessed the growing use of AI-enabled tools in cyber attacks. Notably Imperva blocked an average of 2 million AI-powered cyber-attacks every day.

AI tools such as ChatGPT, ByteSpider Bot, ClaudeBot, Google Gemini, Perplexity AI, Cohere AI, Apple Bot and more are revolutionizing how users interact with their favorite brands, how students learn and how employees perform tasks and create content more quickly than ever before. However, these tools are also being used as a new attack vector.

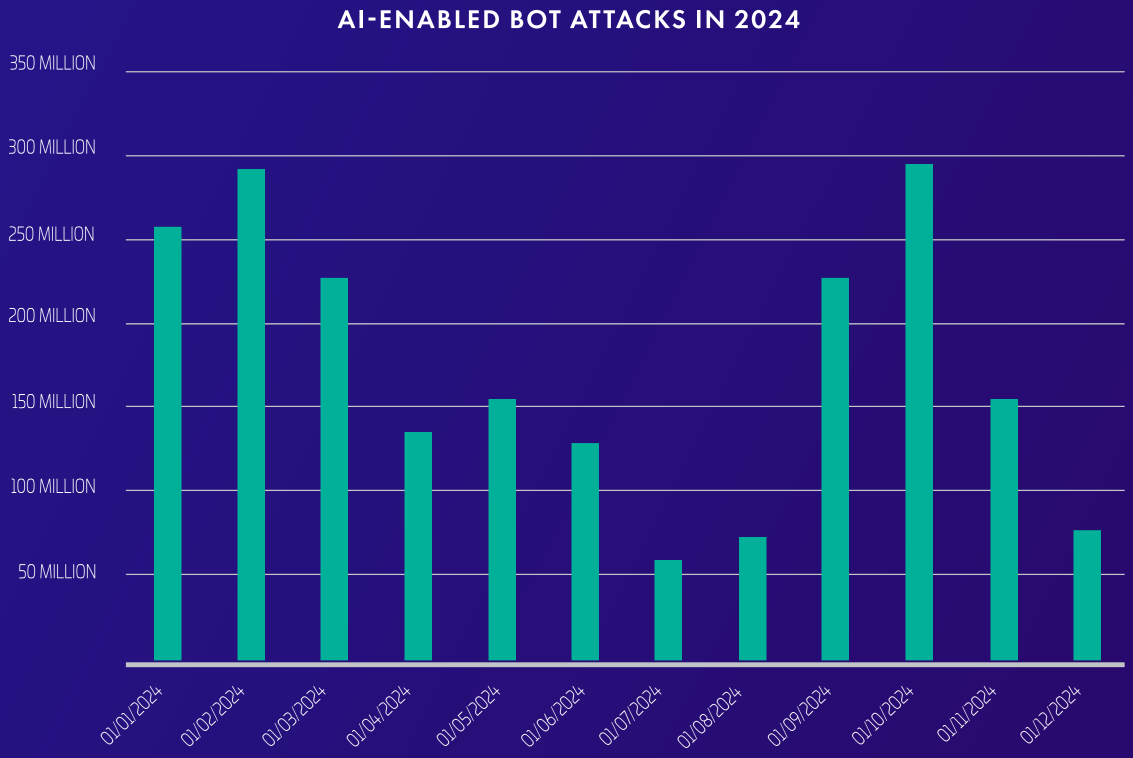
In an analysis of AI tools, the Imperva Threat Research team found that most of the widely used AI-powered tools currently in circulation are being used for cyber-attacks. The distribution of bot attacks across the AI tools analyzed varied significantly. As shown in the chart below, ByteSpider Bot was responsible for 54% of all AI-enabled attacks followed by AppleBot at 26%. ClaudeBot accounted for 13%, while ChatGPT User Bot contributed 6% of the attacks.

ByteSpider's dominance in AI-enabled attacks can largely be attributed to its widespread recognition as a legitimate web crawler, making it an ideal candidate for spoofing. Cybercriminals frequently disguise their malicious bots as web crawlers to evade detection and bypass security measures that whitelist known web crawlers. In contrast, AppleBot (26%) and ClaudeBot (13%) are used less frequently, likely due to stricter security controls or less favorable spoofing potential.

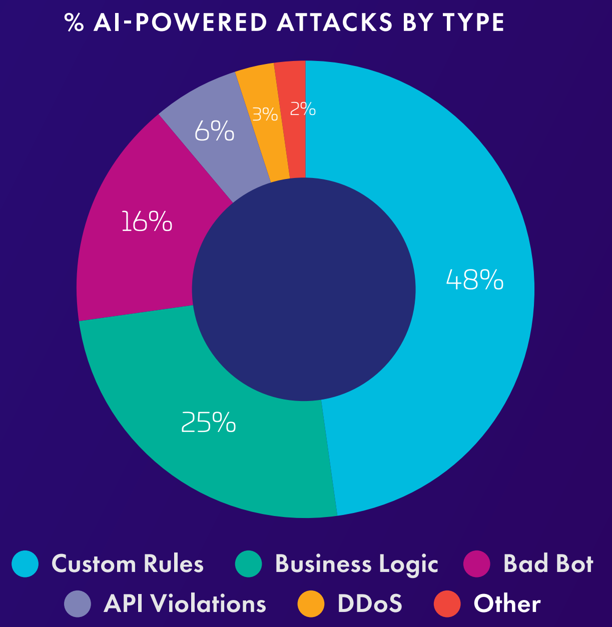
BOT ATTACKS BY AI TOOL



Fluctuations in attack volume throughout the year suggest that attackers are still in an experimental phase, refining their tactics to maximize the effectiveness of these emerging tools. As adversaries continue to adapt, we anticipate this attack vector will expand in the coming years, fueling a rise in automated threats.



AI is enabling attackers to execute a wide range of cyber threats, including DDoS attacks, custom rules exploitation, and API violations. While API violations can involve automated bot activity, they also include broader abuse scenarios, such as unauthorized access attempts and exploitation of misconfigurations. However, bot-driven attacks, in particular, are becoming more sophisticated and harder to detect. In 2024, bad bots accounted for over 16% of all AI-enabled attacks. When combined with business logic attacks—which use automation for stealthy, low-and-slow reconnaissance—this number rises to 41%. This trend highlights how attackers are leveraging AI to refine their techniques, particularly in identifying and exploiting API vulnerabilities to extract sensitive data. As AI capabilities advance, defending against Business Logic Abuse will become even more challenging.



Bot Evasion Tactics

As bots become more sophisticated and mimic human behavior, security teams face increasing challenges in differentiating between automated threats and real users. Additionally, with growing concerns around data privacy, bot operators increasingly use VPNs and obfuscation techniques to blend into legitimate human traffic and avoid being flagged as automated threats.

Based on insights from Imperva's dedicated bot-focused Security Analysts and the Imperva Threat Research team, the following list highlights the latest evasion tactics and techniques employed by bot attackers in 2024:

Fake browser identity and attributes

Many simple bad bots fake their browser identity to appear as a legitimate browser (e.g., Chrome, Firefox). This is a simple but effective way to evade basic security measures. More advanced bots will also fake other browser attributes, such as headers and JavaScript execution to avoid detection by more advanced bot mitigation tools.

Residential Proxies

Attackers use residential IP addresses to evade detection and blend in with normal traffic. Residential proxies allow attackers to route malicious traffic through real user devices, making it harder to detect and block them based on IP reputation alone. While the use of residential ISPs for bot attacks decreased slightly from 26% of all bot attacks where traffic was routed via an ISP in 2023 to 21% in 2024, it remains a favored tactic due to its effectiveness in mimicking legitimate users.

Privacy Tools

Services like iCloud Private Relay mask user identities, increasing the challenge of distinguishing between legitimate human traffic and automated bot activity.

API Abuse

Attackers exploit exposed or unprotected APIs to extract data, automate attacks, and bypass front-end security controls.

App Cracking

Bots target outdated mobile applications that do not enforce mandatory updates, making them vulnerable to reverse engineering, credential stuffing, and unauthorized modifications.

Bypassing CAPTCHA

AI-driven bots solve CAPTCHA challenges with high accuracy, rendering many traditional defenses ineffective.

Property-cycling

AI enables rapid switching of IP addresses, user agents, or browser parameters, to evade detection.

Headless Browsers

Tools like Puppeteer, Playwright, Selenium are enhanced by AI to evade detection and allow attackers to interact with websites just like a human user would execute JavaScript, handle CAPTCHA challenges and navigate pages dynamically.

AI-Assisted Scripting

AI-generated bot scripts increase attack volumes and automation efficiency.

Content Scraping and Anti-detect browsers

Content scraping services such as Browser.ai enable large-scale data extraction, while anti-detection browsers like Multilogin, GoLogin, and AdsPower help evade security measures.

Consistent Token Generation

Bots generate consistent tokens, reducing the chances of triggering anti-bot protections during postback processes.

Polymorphic Bots

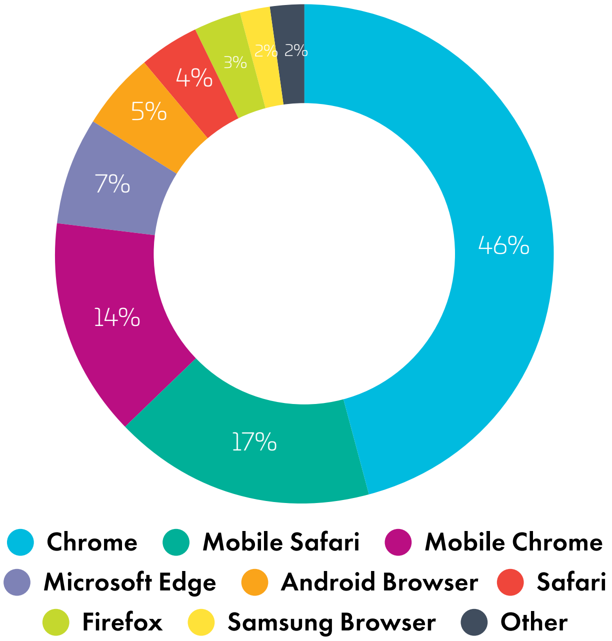
Self-learning bots dynamically change attributes to evade detection.

Bots-As-A-Service (BaaS)

A growing ecosystem of commercialized bot services is driving an unprecedented surge in automated threats across industries.

Browser Impersonation by Bad Bots

TOP BROWSERS IMPERSONATED BY BAD BOTS IN 2024



In their quest to continue undetected, bad bots disguise themselves as popular web or mobile browsers typically used by humans. This is accomplished through browser automation tools. While this was once considered an advanced method of evasion, it has since become a standard approach for many bad bots. Over the years, the browsers favored by these bots have shifted in line with changing human user preferences and evolving strategies to stay under the radar. For instance, Internet Explorer, once widely used by both legitimate users and bad bots, has largely fallen out of favor in recent years.

Chrome remains the top browser that attackers impersonate, as it has done for the last ten years, accounting for 46% of all bad bot attacks in 2024. The percentage of attacks where bots declare themselves as Chrome increased from 40% to 46% in 2024.

Attackers often choose to impersonate Chrome for several legitimate reasons:

Widespread Usage Chrome is the most popular browser globally, used by a significant majority of internet users. By mimicking Chrome, attackers increase the likelihood that their bot traffic will blend in with legitimate user activity, reducing the chances of detection by security systems.

Common Whitelisting Many websites and security systems whitelist traffic from well-known browsers like Chrome, assuming it is legitimate. Since Chrome is widely trusted, bad bots can bypass basic bot mitigation systems that may not scrutinize requests from recognized browsers.

Advanced Capabilities Chrome supports a wide range of modern web technologies (such as JavaScript and HTML5), which many websites rely on.

By impersonating Chrome, attackers can exploit these features to navigate more complex sites, interact with dynamic content, and carry out more sophisticated attacks, like credential stuffing or scraping, without raising suspicion.

Mobile Safari is the second most mimicked browser, accounting for 17% of attacks. Being the default browser on Apple devices, including iPhones and iPads, which have a significant global user base, by mimicking Mobile Safari, attackers can target a large segment of mobile web traffic.

For many of the same reasons **Mobile Chrome** is the third most popular choice for attackers, remaining close to Mobile Safari at a steady 14% year-over-year.

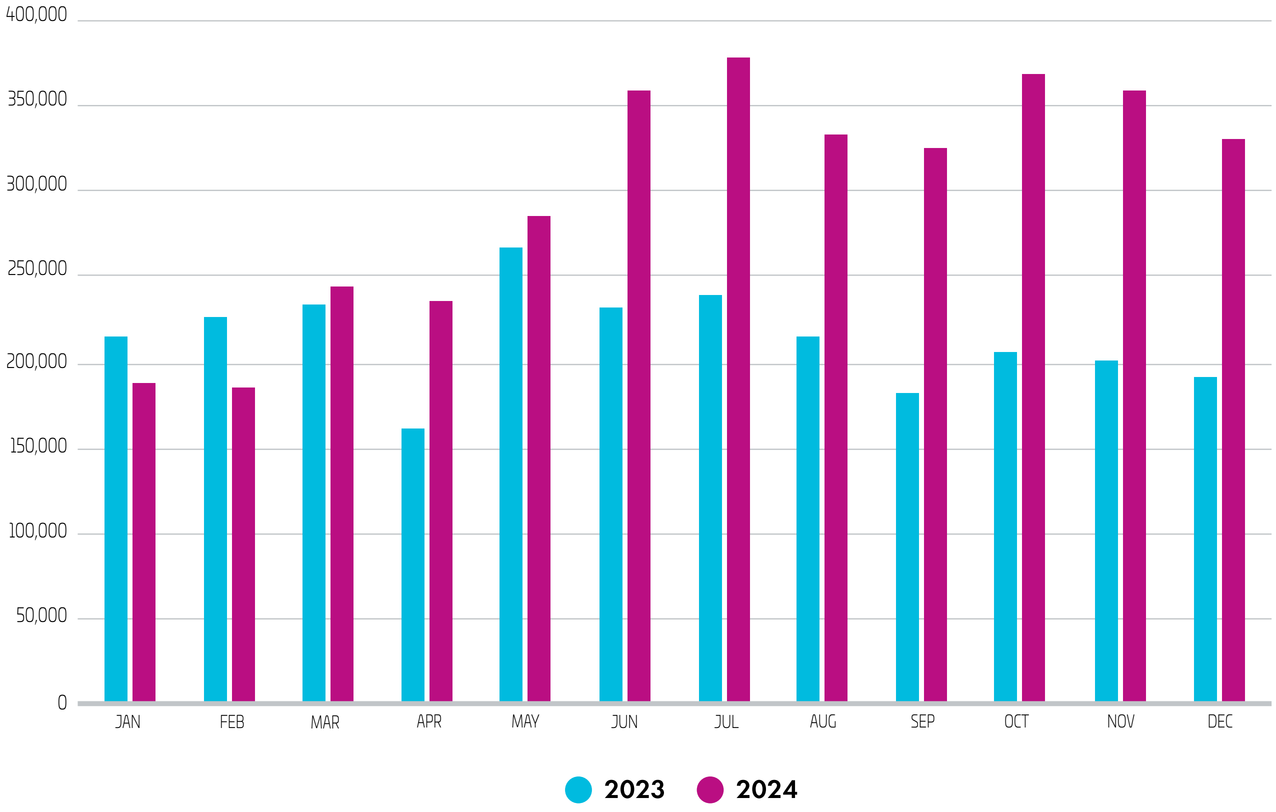
Account Takeover Attacks

Account Takeover (ATO) attacks use malicious bots to gain unauthorized access and take over online user accounts through credential stuffing and credential cracking. These attacks lead to digital identity theft and financial losses for targeted organizations.

ATO attacks are among the most significant cybersecurity challenges facing digital businesses today. A successful attack can result in financial loss, theft of sensitive customer data, misuse of personal information, and reputational damage.

The chart below shows the month-by-month growth of ATO attacks over the past two years. As the chart shows, ATO attacks grew significantly from June onwards with the greatest percentage growth in the months of September, October and November when ATO attacks increased by 79% each month compared to the same period the previous year.

MONTHLY ACCOUNT TAKEOVER ATTACKS 2023 vs 2024



Below are some possible reasons why ATO attacks increased so significantly from June onwards last year:

Seasonal E-commerce and Sales Events

With major shopping events (like Black Friday and holiday sales) starting to peak in the second half of the year, attackers target high-value accounts during these times, contributing to the sharp rise in ATO attempts.

Increased Data Breaches

The rise in compromised credentials from high-profile data breaches has provided attackers with larger databases of stolen login information, making it easier to execute ATO attacks. According to the Identity Theft Resource Center (ITRC), over 1.7 billion data breach notices were issued across the United States in 2024, marking a 312% increase from the 419 million notices sent in 2023.

More Sophisticated Attack Techniques

Attackers are using more advanced tools, such as bots and AI-driven automation, to bypass traditional security measures like CAPTCHA and MFA, leading to a surge in successful ATOs.

Most targeted industries by Account Takeover Attacks

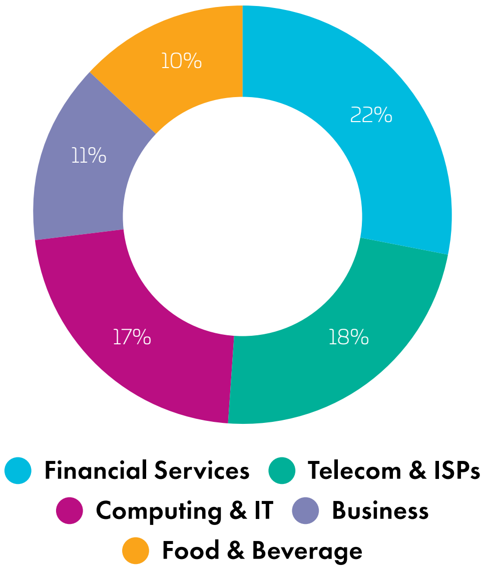
The chart on the right shows the top five most targeted industries for Account Takeover attacks in 2024 accounting for 78% of all attacks.

The top targeted industry was Financial Services accounting for 22% of all ATO attacks, followed by Telecom and ISPs with 18%, and Computing & IT with 17%.

The Financial Services industry has always been a prime target for account takeover attacks because of the high value of accounts and the sensitive nature of the data to be obtained. Banks, credit card companies and fintech platforms hold a vast amount of Personally Identifiable information (PII), including credit card and bank account details which can be sold for a profit on the dark web. The proliferation of APIs in the industry has expanded the attack surface for cyber criminals who target API vulnerabilities such as weak authentication and authorization methods, to conduct account takeover and data theft.

The **Telecom industry** is also a top target for account takeover but motivation that extends beyond financial gain. While access to sensitive PII and customer data can bring financial reward for attackers, the Telecom industry controls critical internet infrastructure and by compromising an internet services provider or ISP's accounts or systems, attackers can intercept our reroute traffic (man-in-the-middle attacks), deploy malware or disrupt services in the case of nation state actors, who often target Telecom organizations for espionage and surveillance in times of geopolitical conflict.

FIVE INDUSTRIES ACCOUNT FOR 78% OF ATO ATTACKS



Consequences of Account Takeover

A successful account takeover attack that results in a data breach can lead to regulatory penalties, legal costs, compensation claims, reputational damage and long-term financial losses. The severity depends on the nature of the breach, the regulatory environment, and the company's response time. Here are some examples of regulatory penalties:

REGULATION	PENALTIES	ADDITIONAL CONSEQUENCES
GDPR **(General Data Protection Regulation)**	Fines up to €20 million or 4% of global annual turnover for failure to protect personal data	Additional penalties for failure to notify authorities within 72 hours
CCPA **(California Consumer Privacy Act)**	Fines up to $2,500 per violation or $7,500 for intentional violations	Consumer lawsuits for personal data exposure, including class-action lawsuits
HIPAA **(Health Insurance Portability and Accountability Act)**	Fines ranging from $100 to $50,000 per violation, with a maximum annual penalty of $1.5 million	Severe penalties for exposing Protected Health Information (PHI)

Bad Bots: A Global Problem

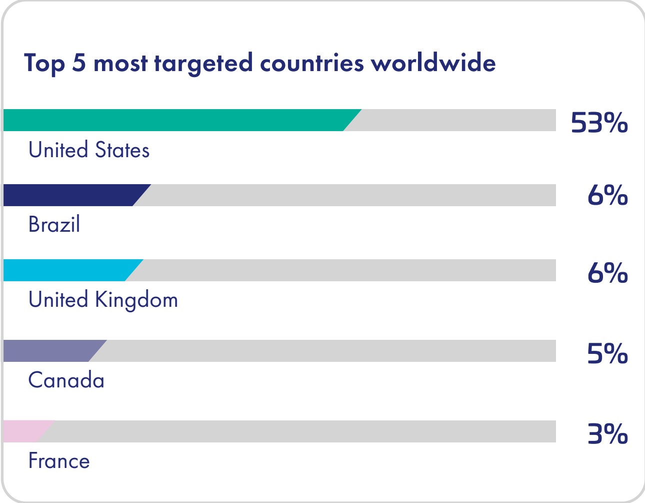
More Than Half of All Bot Attacks Targeted the United States

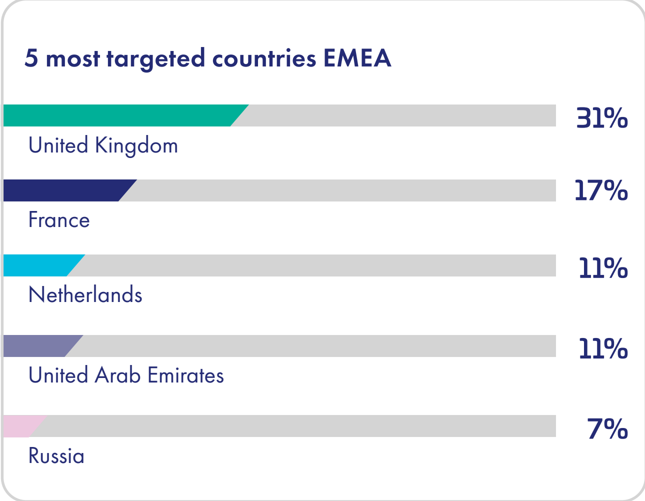
The United States remained the top targeted country for bot attacks accounting for 53% of all attacks in 2024. Brazil and the United Kingdom were joint second with 6% of all attacks targeting them, respectively.

The United States boasts the world's largest online economy, with millions of consumer transactions occurring daily. As home to a significant share of global wealth, leading financial institutions, and tech giants, it presents a highly attractive target for cyber attackers seeking lucrative opportunities.

Almost One-Third of All Bot Attacks in EMEA Targeted UK Sites

In 2024, the United Kingdom was the most targeted country in the Europe, Middle East, and Africa (EMEA) region, accounting for 31% of all bot attacks. Much like the United States, the UK serves as the region's leading financial hub, with a high concentration of wealth, major banks, and fintech companies operating in London. This makes it a prime target for cybercriminals looking to exploit financial transactions, conduct account takeovers, and deploy fraud-related bot attacks.


Top 5 most targeted countries worldwide


5 most targeted countries EMEA

Additionally, geopolitical factors continue to shape the cybersecurity landscape. Notably, Russia and Ukraine both ranked among the top ten most targeted countries in EMEA, highlighting the ongoing cyber threats influenced by regional conflicts. Cyberattacks on these nations often include state-sponsored operations, hacktivism, and financially motivated threats, further underscoring the complex and evolving nature of cyber risks across the region.

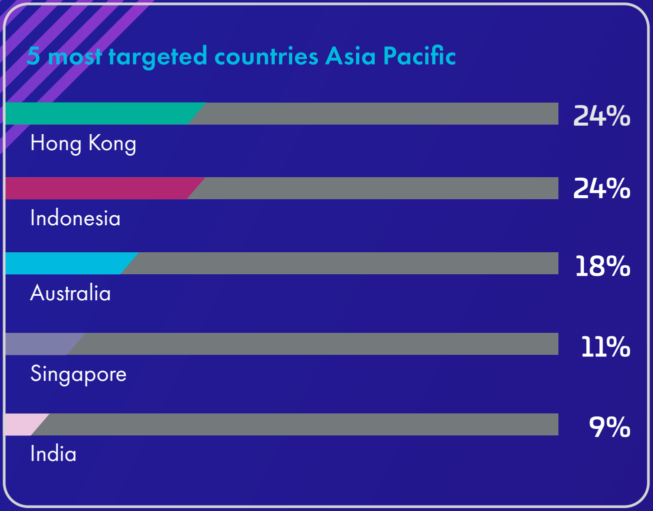
Top Targeted Countries APAC

In 2024, bot attacks in the Asia-Pacific (APAC) region were heavily concentrated in Hong Kong and Indonesia, with each country accounting for 24% of all bot attacks. Together, they made up nearly half of the region's total bot activity.

Hong Kong's status as a global financial hub and a gateway to China makes it a prime target for cybercriminals seeking to exploit banking, fintech, and e-commerce platforms. Meanwhile, Indonesia's large and rapidly growing digital economy, combined with relatively weaker cybersecurity infrastructure, has made it particularly vulnerable to bot-driven fraud and credential stuffing attacks.

Australia followed closely in third place, accounting for 18% of all bot attacks. As one of APAC's most developed economies with a strong financial sector, e-commerce market, and critical infrastructure, Australia remains a frequent target for cybercriminals using bots to launch credential attacks, and automated fraud schemes.

The concentration of attacks in these countries underscores the evolving cyber threat landscape in APAC, where economic growth, digital expansion, and geopolitical factors continue to shape cybersecurity risks.

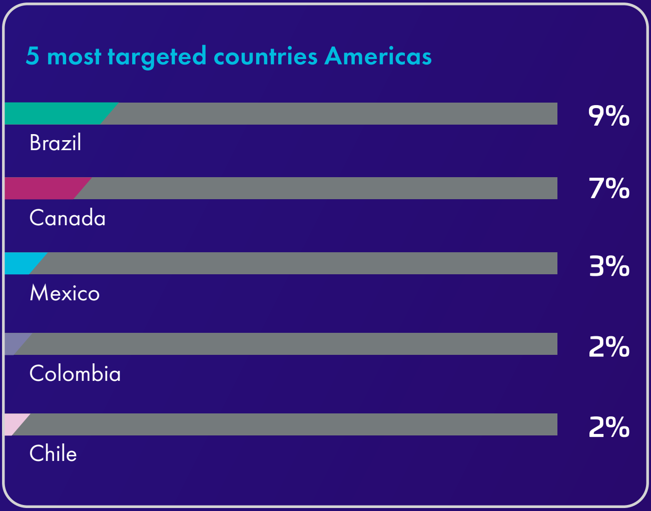


Top Targeted Countries Americas

In 2024, the United States remained the dominant target for bot attacks in the Americas, accounting for a staggering 76% of all incidents. However, outside the U.S., Brazil (9%) and Canada (7%) were the most targeted countries in the region.

Brazil's high ranking could be due to its rapidly growing digital economy, widespread mobile banking adoption, and high levels of online fraud. Cybercriminals often exploit vulnerabilities in Brazil's financial and e-commerce sectors, using bots for credential stuffing and payment fraud. Additionally, Brazil's large population and high internet penetration make it a lucrative target for bot-driven cybercrime.

Canada, ranking third, is a frequent target due to its strong banking sector, e-commerce growth, and digital government services. Bot attacks in Canada often involve account takeovers, automated fraud, and scraping of sensitive data. The country's close economic ties with the U.S. also make it a prime target for cybercriminals looking to exploit cross-border transactions and shared digital infrastructure.



Industry Overview

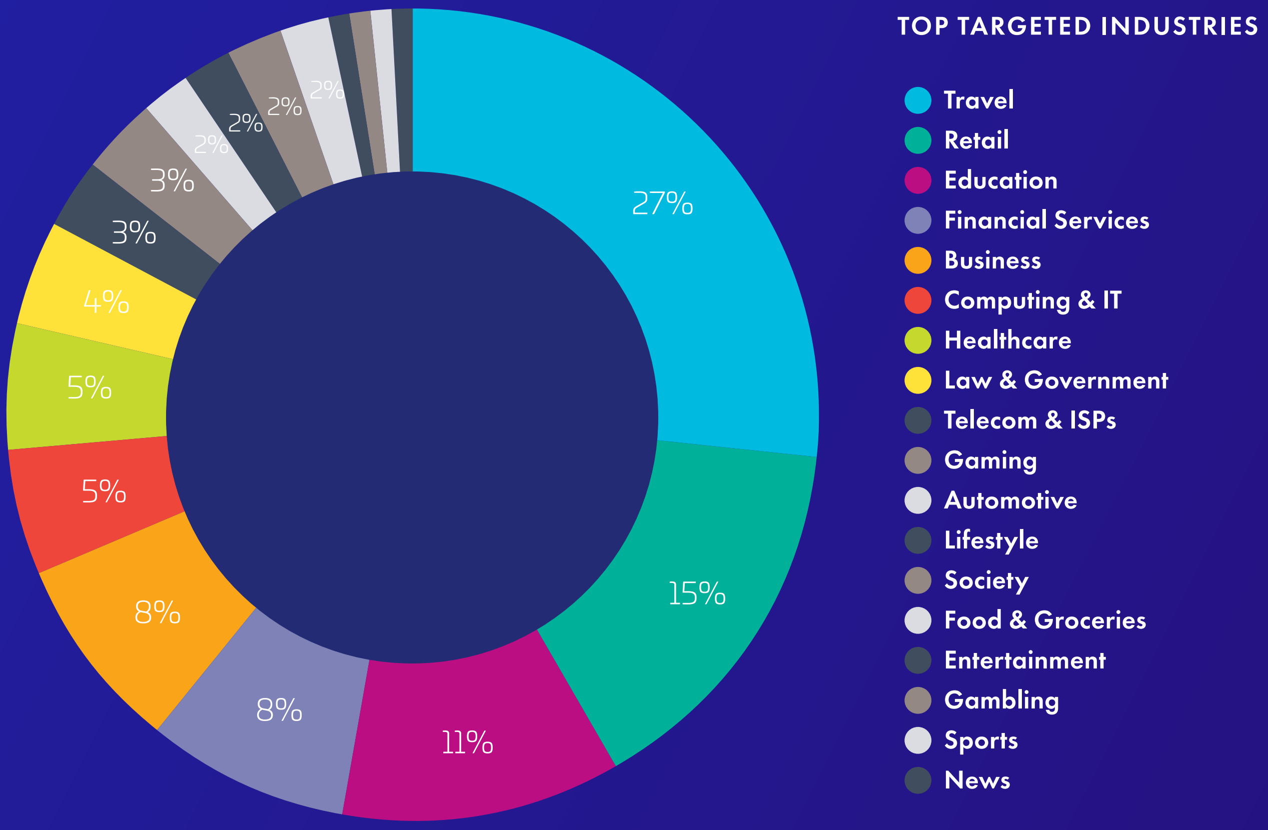
The Top Industries Targeted by Bot Attacks

Travel has bypassed Retail in 2024, accounting for more than a quarter of all bad bot attacks, 27%, to become the most targeted industry for bad bots. Bad bots targeting the Retail sector have dropped significantly from 24% in 2023 to 15% in 2024.

Both the Travel and the Retail sectors face an advanced bot problem with bad bots making up 41% and 59% of their traffic, respectively. We will take a closer look into why bots are targeting these two industries later in the report.

Education has replaced Financial Services as the third most targeted industry with 11% of bad bot traffic targeting Education sites. The Education sector has the highest percentage of simple bot attacks, 92% yet is the third most targeted industry in 2024. This could indicate that the attacks are being launched by less sophisticated attackers with a lower skillset, possibly students with access to GPT tools.

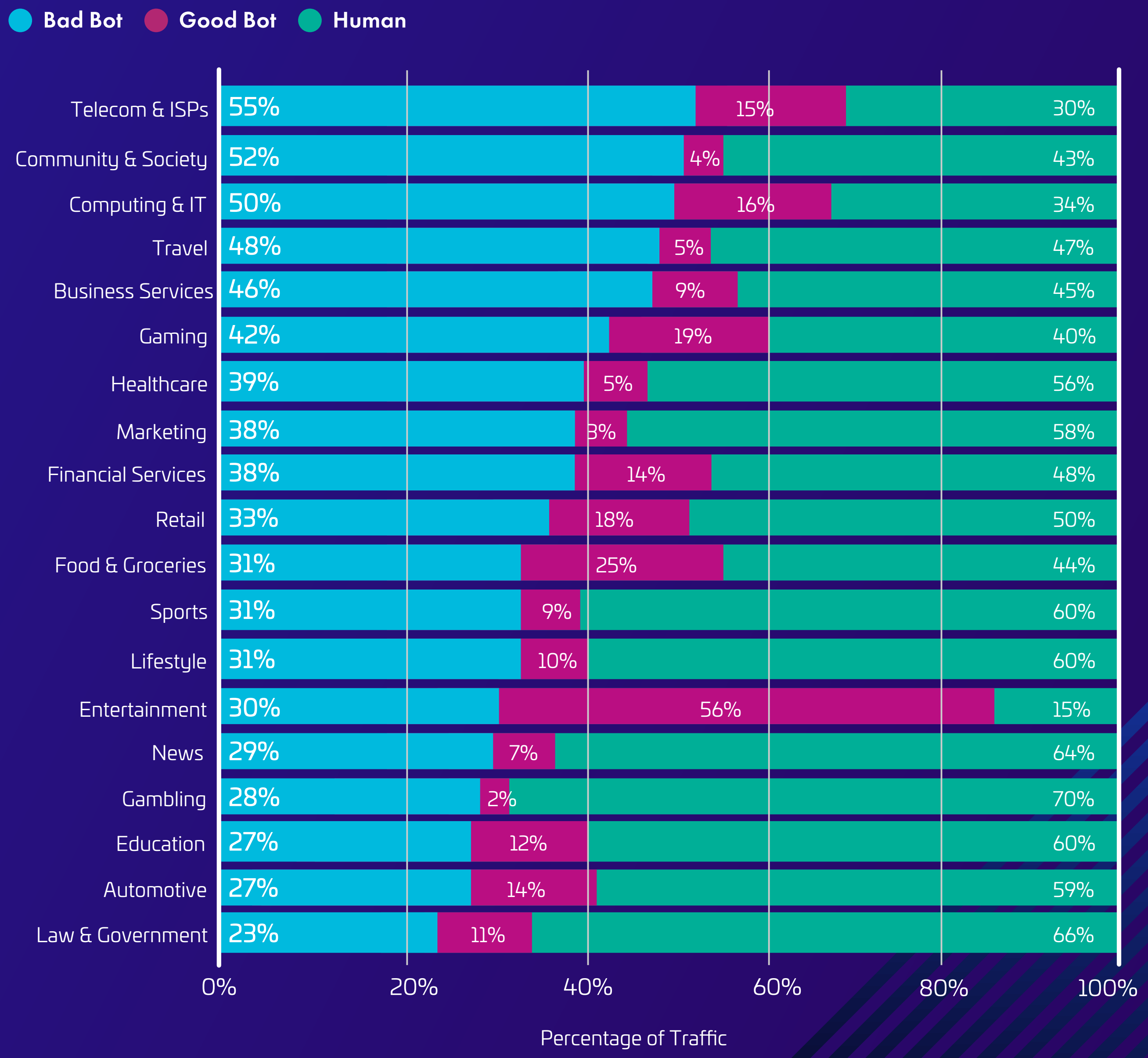
The percentage of bad bot traffic to Financial Services sites has dropped by almost 50% from 16% to 8% since last year.



Bad Bot vs Good Bot vs Human

The following chart provides a breakdown of good bot, bad bot and human traffic to different industries. From the chart we can see that Telecom & ISPs has the highest percentage of bot traffic with 56%. Community & Society is a close second with 52% followed by Computing & IT with 50%.

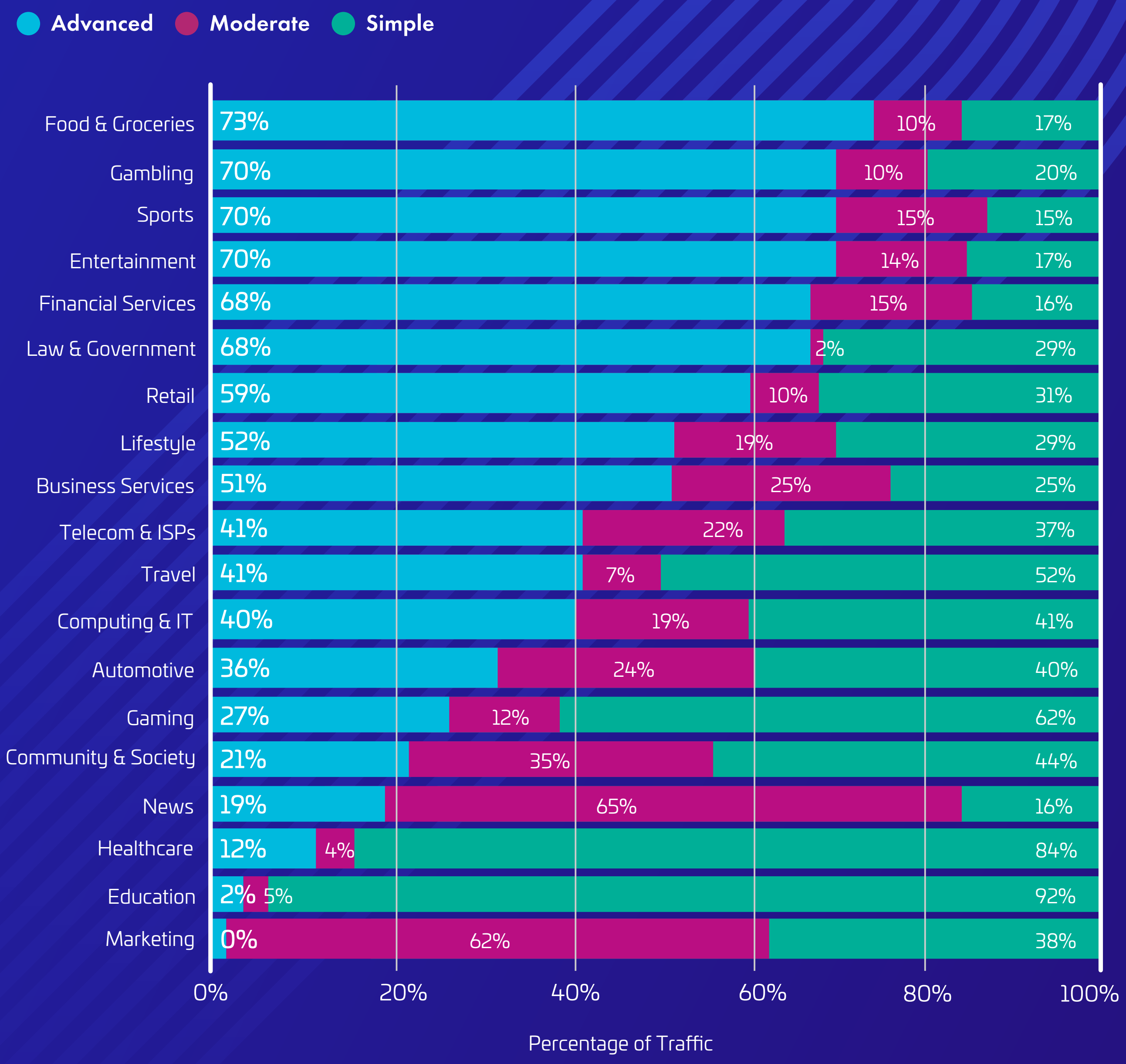
TRAFFIC PROFILE BY INDUSTRY IN 2024



Bot Sophistication by Industry

The previous chart showed bad bot levels for each industry however this alone doesn't give the full risk status of each industry. For example, 31% of traffic to Food and Grocery sites is made up of bad bots, the next chart shows that 73% of bot attacks to this sector are advanced indicating this industry is facing a complex bot problem. The Food and Groceries sector Advanced Bot percentage in 2023 was 50% and has jumped to 73% in 2024. Bots attack online grocery retailers through methods like gift card fraud and inventory scalping.

BOT SOPHISTICATION BY INDUSTRY IN 2024



Bots and the Travel Industry

In 2024, the travel industry became the most attacked sector, accounting for 27% of all bot attacks, up from 21% in 2023, a 6% surge. The most notable shift in 2024 is the decline in advanced bot attacks targeting the travel industry (41%, down from 61% in 2023) and the sharp increase in simple bot attacks (52%, up from 34%). This shift suggests that the AI-powered automation tools that have lowered the barrier to entry for attackers, are making it possible for less sophisticated actors to launch more basic bot attacks. Instead of relying solely on advanced techniques, cybercriminals are deploying large volumes of simpler bots to overwhelm travel sites, making attacks more frequent and widespread.

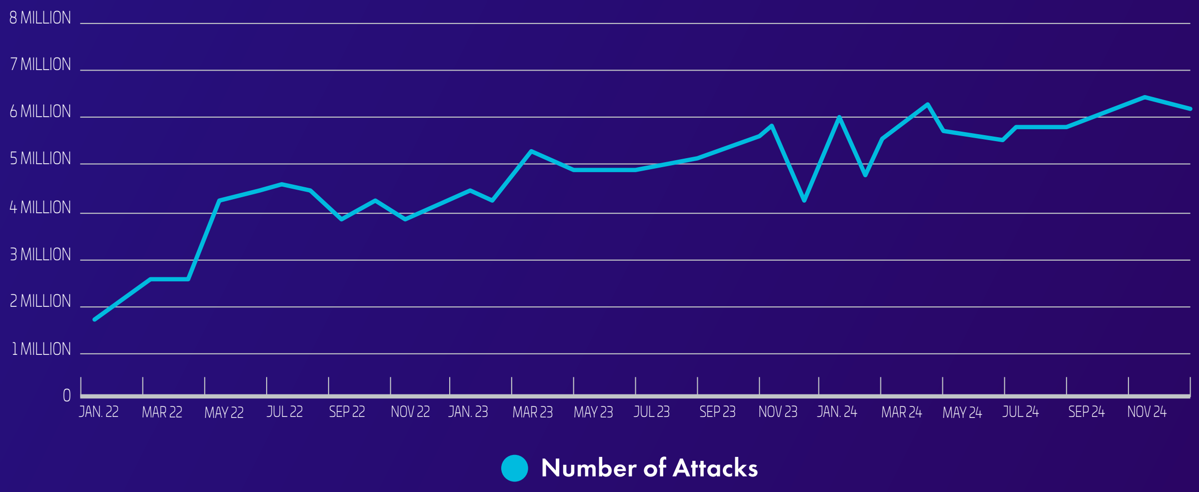
Key Threats Facing the Travel Industry

The travel industry, particularly airlines, faces a range of automated threats that disrupt operations and impact revenue:

- **Seat Spinning** Bots simulate the booking process up to the payment step, holding tickets but never completing the purchase, denying real customers access and forcing them to look elsewhere.
- **Look-to-Book Ratio Distortion** Excessive bot traffic inflates look-to-book ratios, skewing demand and pricing models, putting airlines at a competitive disadvantage.
- **Unauthorized Scraping** Competitors and fraudsters scrape fare data, affecting pricing strategies and revenue management.
- **Loyalty Program Fraud** Bots execute credential stuffing attacks to hijack loyalty accounts and redeem stolen rewards.
- **Ticket Scalping** Attackers use bots to hoard tickets for high-demand flights, reselling them at inflated prices.

The chart below shows the growing number of bot attacks targeting the travel industry over the past 3 years with a 280% rise in bot attacks from January 2022 to December 2024, highlighting the industry's growing vulnerability.

RAPID GROWTH OF BOT ATTACKS TARGETING THE TRAVEL INDUSTRY



Why Bad Bots Are a Retail Nightmare

And they're no longer waiting for peak holiday shopping season

Retail was the second most attacked industry in 2024 (15% of all bot attacks). 33% of web traffic to retail sites was driven by bad bots, up from 26% in 2023. The rise in advanced attacks (59% vs. 52% in 2023) highlights growing sophistication, while moderate (10%) and simple (31%) bot attacks declined slightly.

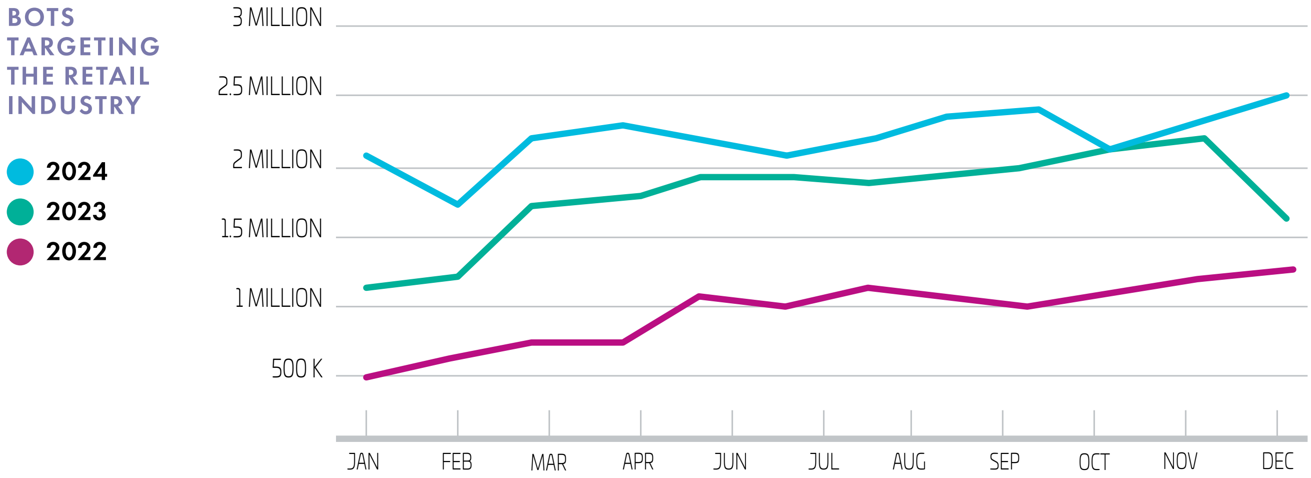
Retailers face threats like scalping, credential stuffing, gift card fraud, price scraping, and DDoS attacks. These attacks peak during the holiday shopping season, disrupting operations and leading to revenue loss, customer trust issues, and increased infrastructure costs. Hackers particularly thrive on marketing campaigns and product launches, where high-value items attract automated attacks, leading to a frustrating customer experience.

According to the Imperva Security Analyst Services team, as website traffic spikes during major sales events, bot traffic increases 2 to 3 times compared to normal days, compounding operational challenges. Cart abandonment bots add products to carts without completing purchases, creating artificial scarcity and distorting supply-demand dynamics.

Bot Attack Trends in the Retail Sector

The chart below illustrates bot attacks targeting the retail sector over the past three years. In 2022 and 2023, attacks increased from March to April, then steadily climbed until November, aligning with peak online shopping periods like Black Friday and Cyber Monday, which continue to attract malicious bots.

In 2024, however, the pattern shifted. Bot traffic spiked around April and September, followed by another increase from October onward. This shift suggests that bots are no longer solely waiting for the holiday shopping season but are targeting retailers at various times throughout the year. The change may also indicate that AI-driven tools are



making bot attacks more accessible, allowing attackers to operate more frequently and opportunistically rather than concentrating efforts around traditional peak shopping events.

Spotlight on the Airline Industry

Unreliable Look-to-Book Metrics - A Pain in the Botside!

Skewing pricing data is a bot's favorite pastime

Airlines are facing a known but growing issue: their look-to-book ratio—the metric airlines use to track ticket searches versus ticket purchases—is being manipulated by scraping bots and create challenges when it comes to competitive pricing.

Look-to-book fraud is a type of malicious bot activity that negatively affects airlines worldwide. These bots flood airline websites, inflating search volume without completing bookings, ultimately skewing demand forecasts, disrupting dynamic pricing models, and increasing operational costs.

Despite the severity of the issue, scraping often flies under the radar as a business problem rather than a security threat. Deploying advanced bot mitigation controls and continuously monitoring traffic restores accurate pricing models, reduces IT strain, and safeguards revenue.

For airlines, ignoring bot-driven look-to-book manipulation puts them at a competitive disadvantage—especially when rivals use bots to scrape fare data and undercut prices. The lesson?

If you don't control your web traffic, someone else will.

> “Bots love to skew pricing data and marketing metrics!”

What is a Bot?

A bot is an automated software application that performs tasks on the internet. Bots can be good, such as search engine crawlers that index content, or bad, such as those used for malicious activities.

What is a Bad Bot?

Bad bots are automated programs designed to perform harmful activities, such as scraping data, spamming, and launching denial-of-service attacks. These bots can mimic human behaviour, making them difficult to detect and block.

CASE STUDY

Marketing Fraud

How Bad Bots Disrupted a Global Marketing Campaign

A leading global talent agency faced a significant challenge with their digital marketing efforts. Despite investing hundreds of thousands of dollars into job advertisements, social media, and targeted ads, the agency saw little to no return on investment (ROI). Their analytics showed high volumes of traffic to their website, but something was off.

Through a thorough analysis, Imperva discovered that a staggering 83% of the website traffic was generated by bad bots. This false traffic skewed their data, making it nearly impossible for them to accurately measure campaign effectiveness. This volume of bot activity, especially in job searches and job postings, was one of the highest seen in the industry, with most agencies experiencing an average of 53%.

The impact was clear: their digital marketing campaigns were being undermined by bot activity, leading to misleading insights and wasted resources.

In just under four days, Imperva's Advanced Bot Protection (ABP) solution fully blocked the bad bot traffic, allowing the agency to regain control of their data and start seeing real, actionable results from their marketing campaigns. Despite the bot operators' attempts to evade our protection system, Imperva's solution proved highly effective in mitigating the threat, safeguarding the agency's content, and ensuring the integrity of their campaigns. With 100% of bad bot activity blocked, the agency was finally able to experience the true value of their marketing efforts, seeing a significant improvement in their ROI and more reliable insights for future strategies.

> **Bad bots drain marketing budgets and crush ROI expectations**

Recommendations

Businesses need to take steps to protect themselves from bots and online fraud. Since each site has its own specific vulnerabilities and potential attack vectors, a one-size-fits-all solution can be difficult to find. However, adopting a proactive approach with a range of security measures can significantly reduce the risks. This includes using advanced bot detection tools and effective cybersecurity management solutions. Together, these strategies create a robust defense against the constantly changing landscape of bot-related threats.

APIs have become a critical attack surface in modern digital infrastructure, frequently targeted for credential stuffing, data scraping, and automated exploitation. To ensure comprehensive protection, specific recommendations addressing API security are included below.

1. Risk Identification

Stopping bot traffic begins with identifying potential risks to your website:

A. Marketing and eCommerce initiatives often attract an increased presence of bots, particularly during the launch of limited-quantity, high-demand products. Whether the latest sneakers, next-gen gaming consoles, or exclusive collector's items, specifying a launch date for these coveted products is a beacon for bots. These automated entities aim to secure the merchandise before genuine customers can, potentially monopolizing access and undermining your sales efforts. It's crucial to fortify your website's defenses to effectively manage the surge in traffic, ensuring you can distinguish between legitimate consumers and evasive bots intent on hijacking the product launch. Implementing advanced traffic analysis, real-time bot detection mechanisms and robust authentication measures can help safeguard your platform, ensuring fair access for actual customers.

B. Recognizing potentially exploitable website and application functionalities on your site is a crucial element of an effective bot management strategy. Certain website features are particularly susceptible to malicious bot activities. For instance, incorporating login capabilities can lead to Credential Stuffing and Credential Cracking attacks, where attackers use stolen credentials to gain unauthorized access. Similarly, the presence of a checkout form can escalate the risk of credit card fraud, known as Carding or Card Cracking. Furthermore, implementing gift card functionalities can attract bots intent on committing fraud. To mitigate such risks, it is essential to apply enhanced security measures and enforce stricter rules on these pages. Implementing multi-factor authentication, CAPTCHAs, and continuous monitoring for suspicious activities can significantly strengthen your site's defenses against these automated threats. Leveraging AI-driven detection systems enhances real-time identification of sophisticated bot activity. Adaptive CAPTCHA mechanisms and dynamic rate-limiting techniques are particularly effective in neutralizing bots that attempt to bypass standard security measures.

C. Additionally, Identify your most critical and frequently targeted paths—such as login pages, checkout workflows, and API endpoints—and apply mitigation techniques like rate limiting, monitoring high-request IPs, and securing the entire path hierarchy. Since APIs are often targeted by bot-driven credential stuffing and data scraping attacks, implementing API-specific rate limiting, authentication hardening, and anomaly detection can further protect against unauthorized access and abuse.

2. Vulnerability Reduction

Securing exposed APIs and mobile applications is just as important as website security, highlighting the need for a holistic cybersecurity strategy that covers all digital touchpoints. APIs and mobile apps often serve as gateways to sensitive data, creating additional vectors for cyber threats. Implementing robust security measures across all platforms and blocking between systems reduces vulnerabilities, ensuring unified defense against unauthorized access.

API security should enforce authentication best practices and strict access controls to prevent token abuse and unauthorized data scraping. Additionally, multi-layered bot mitigation techniques, such as proof-of-work mechanisms and tarpit strategies, can slow down bots while maintaining a seamless user experience.

3. Threat Reduction: User-Agents

Many bot tools and scripts contain user-agent strings with outdated browser versions. In contrast, humans are forced to auto-update their browsers to newer versions. Take steps to block outdated browser versions:

	BLOCK End of Life more than three years	**CAPTCHA** End of Life more than two years
CHROME VERSION	<100	<110
FIREFOX VERSION	<95	<105
SAFARI VERSION	<13	<14
INTERNET EXPLORER VERSION	<11	<13

Additionally, enforce acceptable reference lists, including geo-fencing, request methods, URL access control, user-agent limitations, and app versioning, to minimize abuse from outdated or illegitimate traffic sources.

4. Threat Reduction: Proxies

The use of proxy services by malicious bots to obscure their activities is on the rise, as attackers employ these services to simulate legitimate user behavior. By leveraging IP rotation from bulk IP services, they can mask their true origins, complicating detection efforts. A strategic approach to mitigating this threat involves restricting access from known bulk IP data centers, significantly reducing the potential for botnet traffic to infiltrate your network. Notable sources of such proxy-based attacks include data centers and cloud service providers, such as Host Europe GmbH, Dedibox SAS, Digital Ocean, OVH SAS, and Choopa, LLC. Implementing access controls and monitoring for traffic originating from these entities can enhance your security posture by preemptively identifying and blocking bot-generated traffic, thereby minimizing the risk associated with these proxy-enabled attacks.

5. Threat Reduction: Automation

Modern tools like Puppeteer, Selenium, and WebDriver are often misused by attackers to imitate human actions online, enabling them to carry out harmful activities such as bulk account registrations and data theft. Distinguishing these malicious efforts from legitimate traffic requires implementing detection strategies for signs of automation, such as unnaturally fast interactions or abnormal browsing patterns. By homing in on these behaviors, organizations can effectively spot and stop automated attacks, safeguarding genuine user interactions.

APIs are especially vulnerable to automated bot abuse, as attackers use headless browsers and scripts to interact with endpoints at scale. Monitoring API traffic for suspicious behavior can help differentiate between legitimate users and automated threats.

To mitigate these threats efficiently, prioritize handling basic bots like automated tools and headless Chrome as quickly as possible.

6. Evaluate Traffic - general bot detection and baselining traffic patterns.

Identifying bot traffic without explicit indicators poses a challenge, yet specific patterns often hint at their presence. High bounce rates and low conversion rates can be telltale signs of non-human traffic. Additionally, sudden unexplained spikes in traffic or an unusually high number of requests targeting a specific URL frequently signal bot activity. Monitoring for these anomalies enables organizations to flag potential bot traffic, facilitating further investigation and appropriate response measures to mitigate unwelcome interference.

Define a baseline for expected traffic patterns and monitor for unexpected deviations that may indicate bot activity. The sudden surge in traffic to a particular endpoint might indicate bots targeting a specific event or operation. To assess whether this spike is bot-driven, analyze the source of this increased traffic.

Look for patterns such as a single IP address, an ISP, or a specific URL generating traffic levels significantly above the norm. Identifying these sources can provide clear evidence of bot activity, enabling you to take targeted action. For example, if traffic predominantly originates from a single IP or a narrow range of IPs, it's a strong indicator of automated access attempts. Such insights are crucial for deploying effective countermeasures against bot attacks, ensuring your digital assets are still protected.

7. Monitor Traffic - real-time monitoring, alerting, and API-specific threats.

Define your failed login attempt baseline on login pages, then monitor for anomalies or spikes. Set up alerts so you're automatically notified if any occur. Advanced "low and slow" attacks don't trigger user or session-level alerts, so be sure to set global thresholds. On checkout and gift card validation pages, an increase in failures, or even traffic, can be a signal of carding attacks or that bots such as GiftGhostBot are attempting to steal gift card balances. This includes tracking API request frequency, detecting sudden spikes in API calls, and leveraging behavioral analytics to identify abnormal access patterns that could indicate automated abuse.

8. Awareness and Multi-Factor Authentication (MFA)

Maintaining vigilance regarding global data breaches and leaks is essential. The simplicity with which attackers can purchase credential dumps from these breaches or rent bot infrastructure to automate attacks elevates the threat to a tangible risk. Bots frequently exploit freshly compromised credentials to conduct stuffing attacks and account takeovers (ATO) since these credentials are likely still active. This tactic significantly raises the odds of successfully breaching user accounts on your platform. Staying informed about such breaches and understanding their implications can help you proactively strengthen your defenses, reducing the likelihood of your site becoming a target for these automated threats.

To further protect against unauthorized access, MFA enforces logins, payments, and password resets to add an additional layer of security against automated credential-based attacks. For APIs, enforcing strong authentication mechanisms can help mitigate credential stuffing and token abuse attacks.

9. Evaluate Bot Protection solutions

Evaluating bot protection solutions is crucial as the landscape of bot attacks has significantly transformed. The simplistic measures once sufficient to fend off malicious bots are now ineffective. The insights gathered in this report underscore that the sophistication and adaptability of modern bots surpass previous levels, with their ease of use and effectiveness making them a favored tool among cybercriminals. These bots rapidly evolve, rendering traditional detection methods obsolete, but they also mimic human behavior more closely than ever, making it challenging to distinguish them from legitimate users. In this environment, where attackers leverage bots for their high reward and low-risk benefits, attempting to counteract these threats single-handedly is nearly impossible.

The need for a dynamic defense strategy is more pressing than ever. It's not just about identifying malicious bots; it's about differentiating them from beneficial ones amidst their increasing complexity.

A comprehensive bot prevention solution should incorporate a layered defense approach, including user behavior analysis, profiling, and fingerprinting. Additionally, AI/ML-driven tools should be employed to enhance bot detection accuracy and continuously adapt to evolving threats.

By maintaining continuous vigilance, conducting regular audits, and expanding AI/ML integration, organizations can proactively protect their critical assets against automated threats while balancing false positives and false negatives effectively.

Such a nuanced approach demands the expertise of a dedicated team capable of evolving your defenses at the pace of emerging threats.

10. Don't Play All Your Cards at Once

Implementing all mitigation techniques simultaneously across your entire platform can inadvertently reveal your full defensive playbook, allowing attackers to analyse and circumvent your countermeasures over time.

Instead, organizations should take a strategic, event-driven approach. Reserve specific mitigation techniques for critical moments—such as product launches, major sales events, or high-traffic periods—when bot activity is expected to spike.

Once the event concludes, disable or adjust these controls to prevent attackers from studying and adapting to them.

For APIs, this means dynamically adjusting rate limits, access controls, and bot detection mechanisms based on traffic patterns and risk levels, preventing attackers from identifying and exploiting static defenses.

This approach ensures that your defenses remain unpredictable, making it harder for bots to learn, adapt, and evade detection. By treating bot mitigation as a continuously evolving strategy rather than a static set of rules, organizations can stay one step ahead in the ongoing battle against automated threats.

Appendix

Definitions

What is a bot?

In the context of the internet, a bot is a software application that runs automated tasks. Such tasks can range from simple actions like filling out a form to more complex functions like scraping a website for data.

What is a bad bot?

Bad bots are software applications that perform automated tasks with malicious intent. These bots can extract data from websites without permission to reuse it and gain a competitive advantage. They are often used for scalping, which involves obtaining limited availability items and reselling it at a higher price. Bad bots can also be used to create distributed denial-of-service (DDoS) attacks targeted at the application. Some bad bots undertake criminal activities such as fraud and outright theft. One example is bots that perform credential stuffing, one of the most prominent types of bot attacks. The Open Web Application Security Project (OWASP) provides a comprehensive list of 21 bot attacks in its Automated Threat Handbook1.

What is the difference between good and bad bots?

Not all bots found on the internet are bad. There are also good bots that serve valuable functions. For instance, some bots index websites for search engines or monitor website performance. Googlebot and Bingbot are examples of search engine crawlers that help create and maintain a searchable index of web pages. By indexing web pages, these bots help people find the most relevant sets of websites that match their queries. Such bots are essential for online businesses, allowing potential customers to easily find and access their websites, products, and services.

Even good bots can be a cause for concern

Good bots can significantly impact web analytics reports, as they can make certain pages appear more popular than they are. For instance, a good bot might generate an impression for a page on your website that you advertise, but that ad click never leads to the sales funnel. This can result in lower performance for advertisers and lead to skewed marketing analytics, ultimately leading to incorrect decision-making. Therefore, it is crucial to accurately distinguish between traffic generated by legitimate human users, good, and bad bots, to make informed business decisions.

What is an AI-Powered Bot?

An AI-powered bot uses machine learning and artificial intelligence to mimic human behavior, allowing it to adapt and improve its tactics over time. These bots can analyze data, learn from interactions, and evade traditional detection methods by appearing more like legitimate users.

What is a Polymorphic Bot?

A polymorphic bot is designed to constantly change its appearance and behavior to evade detection, often by altering its code, user-agent, or IP address. This adaptability allows it to bypass security measures by resembling different types of legitimate traffic during each attack.

Bad bot classification

Imperva created the following classification system that categorizes bad bots by their level of sophistication:

- **Simple** Connecting from a single, ISP-assigned IP address, this bot connects to sites using automated scripts. This bot doesn't self-report as a browser.
- **Moderate** This more complex bot uses "headless browser" software that simulates browser technology, including the ability to execute JavaScript.
- **Advanced** The most sophisticated of bots emulates human user behavior like mouse movements and clicks to spoof bot detection. They use browser automation software, or malware installed within real browsers, to connect to sites.
- **Evasive** Sophisticated bot operators are very determined and persistent. If a bot management solution blocks them today, they will likely figure out why they were stopped and return tomorrow with a new technique to evade detection. These actors are using advanced bad bots, which are becoming more challenging to detect due to the advancements in evasion techniques. They often employ various techniques shared between Moderate and Advanced bad bots.

Evasive bots use complex tactics like cycling through random IPs, entering via anonymous proxies, using residential proxies, changing their identities, mimicking human behavior, delaying requests, and defeating CAPTCHA challenges. They use a "low and slow" approach to avoid detection and carry out significant attacks using fewer requests. This method reduces the "noise" generated by many bad bot campaigns, making it difficult to detect them.

Bad Bot Use Cases

BAD BOT PROBLEM	WHAT IS IT	HOW IT HURTS THE BUSINESS	SYMPTOMS	TARGETED INDUSTRIES
Price Scraping	The use of bots to illegally monitor and track pricing information, typically in order to undercut rivals and boost sale	Loss of sales to competitors that scrape your prices, undercut them and beat you in the marketplace Damaged reputation due to scraped data being used in a way that misrepresents the business's prices or products The lifetime value of customers worsens Impacts website performance	Declining conversion rates Your SEO rankings drop Unexplained website slowdowns and downtime (usually caused by aggressive scrapers)	All businesses that show pricing: • Retail • Gaming • Airlines • Travel
Content Scraping	The use of bots to extract content and data from a website	Loss of revenue due to your business's content or data being published elsewhere, leading to fewer people visiting the original site or purchasing your products or services Duplicate content damages your SEO rankings Damage to brand reputation	Your content appears on other sites Your SEO rankings drop Unexplained website slowdowns and downtime (usually caused by aggressive scrapers)	Similar to Price Scraping, but in addition: • Job boards • Classifieds • Marketplaces • Finance • Ticketing
Account Takeover (aka Credential Stuffing, Credential Cracking)	The use of bots to gain illegal access to user accounts belonging to someone else. Usually achieved using brute force login techniques such as Credential Stuffing or Credential Cracking	Direct impact on brand loyalty and reputation, negative PR Customer frustration due to account lockout, data theft or dealing with fraudulent, increasing churn Impacts website performance, availability and reliability Risk of noncompliance with data privacy regulations Increased support and fraud costs	Increase in failed login rates Increase in customer account lockouts and customer service tickets Increase in fraud (lost loyalty points, stolen credit cards, unauthorized purchases) Increase in chargebacks	Any business with a login page
Account Creation (aka Account Aggregation, New Account Fraud)	The use of bots to automate bulk account creation. These accounts can then be misused to perform various forms of fraud, spam content, or spread propaganda	Decreased credibility of certain platforms and websites to bot accounts that are used to spam messages or amplify propaganda Loss of revenue to bots that exploit new account promotion credits (money, points, free plays) Metrics based on the number of user accounts or social media interactions that all originate from bots may lead to poor decision making	Abnormal increases in new account creation Increased comment spam Drop-in conversion rates from new accounts to paying customers	Messaging platforms • Social media • Dating sites • Communities Sign-up promotion abuse • Gaming • Finance

BAD BOT PROBLEM	WHAT IS IT	HOW IT HURTS THE BUSINESS	SYMPTOMS	TARGETED INDUSTRIES
Credit card fraud (aka Carding, Card Cracking)	The use of bots to mass-verify the validity of stolen credit card numbers or guess the missing details (CVV, expiration date, etc.)	Financial losses due to the business's liability for any fraudulent activity that occurs on their platforms: from costly chargebacks to lost revenue due to decreased consumer trust Damaged brand reputation Damages to the fraud score of the business Increased customer service costs to process fraudulent chargebacks Noncompliance with data privacy regulations (PCI-DSS, GDPR, etc.)	Rise in credit card fraud Increase in customer support calls Increased chargebacks processed	Any site with a payment processor: • Retail • Nonprofit/Charities • Airlines • Travel • Ticketing • Finance • Gaming
Denial-of-Service	The use of bots to overwhelm a website with requests, leading to an exhaustion of resources such as file system, memory, processes, threads, CPU, and human or financial resources	Slows the website performance causing brownouts or downtime Lost revenue from the unavailability of websites Damaged brand reputation Potential customer churn	Abnormal and unexplained spikes in traffic on particular resources (login, signup, product pages, etc.) Increase in customer service complaints	All industries
Gift Card Balance Checking and Abuse	The use of bots to automate the enumeration of potential gift card numbers against balance checking pages to steal gift card balances	Like credit card fraud, gift card fraud leads to financial losses due to bots that steal money from gift cards Increased customer service costs to process fraudulent chargebacks Poor customer reputation and loss of future sales Damaged brand reputation	Spike in requests to the gift card balance page Increase in customer service calls about lost balances	Any business offering gift cards as a payment option - Retail predominantly
Denial of Inventory	The use of bots to hold items in shopping carts without ever actually completing the purchase, thus denying them from legitimate consumers	Loss of revenue from unsold items that are held in shopping carts by bots Lower conversion rates Increased cart abandonment rates Damaged customer reputation because unscrupulous middlemen hold all inventory until resold elsewhere	Increase in abandoned items held in shopping carts Decrease in conversion rates Increase in customer complaints about lack of availability of inventory	Businesses offering scarce or time-sensitive items: • Airlines • Tickets • Retail • Healthcare

Bad Bot Use Cases

BAD BOT PROBLEM	WHAT IS IT	HOW IT HURTS THE BUSINESS	SYMPTOMS	TARGETED INDUSTRIES
Scalping	The use of bots to gain an unfair advantage over legitimate consumers and obtain limited-availability and/or preferred goods/ services	Damaged customer reputation Slows the website performance causing brownouts or downtime, leading to loss of revenue Lower lifetime value (LTV), because a bot doesn't regularly come back for additional items Lower average basket value (ABV), because bots target a single product as opposed to legitimate consumers that tend to purchase additional items	Unexplained website slowdowns and downtime (usually caused by aggressive scalping bots) Decrease in conversion rates Increase in customer complaints about lack of availability of inventory	Similar to Denial of Inventory: • Airlines • Tickets • Retail E.g. sneakers, consoles, computer hardware, limited edition items. • Healthcare
Seat Spinning	Bots hold seats without making a payment, often for up to 24 hours	Loss of revenue for unsold seats Reputation damage because legitimate consumers cannot book desired flights	As departure time approaches, seemingly fully booked flights are suddenly showing increasing numbers of empty seats	Airlines

Bad Bots By Industry

INDUSTRY	WHAT BUSINESSES ARE INCLUDED?	WHAT ARE BAD BOTS DOING?
Automotive	Car rentals, manufacturers, dealerships, vehicle marketplaces	Price scraping, data scraping, inventory checking
Business Services	Real estate, third party vendors like retail platforms, CRM systems, business metrics	Attacks targeting APIs, data scraping, account takeover
Computing & IT	IT services, IT providers, services and technology providers	Account takeover, scraping
Education	Online learning platforms, schools, colleges, universities	Account takeover for students and faculty, class availability, scraping proprietary research papers and data
Entertainment	Streaming services, ticketing platforms, production companies, venues	Account takeover, price scraping, inventory scraping, scalping
Financial Services	Banking, insurance, investments, cryptocurrency	Account takeover, carding, card cracking, custom content scraping
Food & Groceries	Food delivery services, online grocery shopping, food & beverage brand sites	Credit card fraud, gift card fraud, account takeover, coupon guessing
Gambling	Casinos, sports betting	Account takeover, odds scraping, account creation for promotion abuse

INDUSTRY	WHAT BUSINESSES ARE INCLUDED?	WHAT ARE BAD BOTS DOING?
Gaming	Online gaming, video games	Account takeover, account creation for promotion abuse and cheating, gaming automation, denial-of-service
Government	Law & government websites, citizen services, states, municipalities, metropolitans	Account takeover, data scraping of business registrations listings, voter registration, appointment scraping and scheduling
Healthcare	Health services, pharmacies	Account takeover, content scraping, "helpful" bots that scrape for appointment availability
Lifestyle	Lifestyle magazines, blogs	Proprietary content scraping
Marketing	Marketing agencies, advertising agencies	Proprietary content scraping, ad fraud, denial-of-service, skewing
News	News sites, online magazines	Proprietary content scraping, ad fraud, comment spam
Retail	eCommerce, marketplaces, classifieds	Account takeover, scalping, denial of inventory, credit card fraud, gift card fraud, data and price scraping, analytics skewing
Community & Society	Nonprofits, faith and beliefs, romance and relationships, online communities, LGBTQ, genealogy	Content and data scraping, account takeover, account creation, testing stolen credit cards on donation pages
Sports	Sports updates, news, live score services	Data scraping (live scores, odds etc.)
Telecom & ISPs	Telecommunications providers, mobile ISPs, hosting providers	Account takeover, competitive price scraping
Travel	Airlines, hotels, holiday booking	Price and data scraping, skewing of look-to-book ratio, denial-of-service, price scraping, account takeover, seat spinning

About the Imperva Bad Bot Report

The 12th Annual Imperva Bad Bot Report explores the rapidly changing landscape of automated internet traffic, examining the increasing sophistication of bad bots and their impact on businesses. Based on invaluable insights from our Threat Research and Security Analyst Services (SAS) teams, this report highlights the latest tactics, techniques, and procedures (TTPs) of malicious bots.

Our analysis draws from data collected from across the Imperva global network in 2024, including the blocking of 13 trillion bad bot requests across thousands of domains and industries. This dataset provides key insights into bot activity to help organizations understand and address the growing risks of automated attacks.

This year's report focuses on the growing role of Artificial Intelligence (AI) in bot attacks, significantly increasing their volume, accessibility, and ability to evade detection. Bad bots are increasingly targeting businesses through tactics like data scraping, account hijacking, and inventory manipulation for financial gain. As AI evolves, organizations must adopt advanced mitigation strategies to protect against fraud, financial losses, and security risks.

These attacks can degrade customer service, inflate prices, and limit access to products, ultimately eroding trust and loyalty. The report also provides actionable recommendations for organizations to defend against this growing threat.

About Imperva Application Security

Imperva is the cybersecurity leader that helps organizations protect critical applications, APIs, and data anywhere, at scale, and with the highest ROI. The Imperva Application Security Platform stops the most advanced attacks with the highest efficacy while minimizing false positives. Its high efficiency enables organizations to quickly onboard, protecting their assets at scale. With the help of the Imperva Threat Research team and our global intelligence community, we stay ahead of the evolving threat landscape, seamlessly integrating the latest security, privacy, and compliance expertise into our solutions.

The Imperva Application Security Platform combines best-of-breed solutions that bring defense-in-depth to protect your applications wherever they live — in the cloud, on-premises, or a hybrid configuration:

- On-Prem and Cloud Web Application Firewall (WAF) solutions for blocking the most critical web application security risks.
- API Security for continuous protection of all APIs using deep discovery and classification.
- Advanced Bot Protection for safeguarding websites, mobile applications, and APIs against today's most sophisticated automated threats.
- Client-Side Protection for safeguarding websites against client-side attacks and streamlining regulatory compliance with PCI DSS 4.0.
- DDoS protection for websites, networks, and DNS to ensure business continuity with guaranteed uptime.
- Content Delivery Network for securely delivering applications worldwide with superior speed and performance.

Start your Application Security Free Trial today to protect your applications from bad bots.

imperva
a Thales company

Contact us

For all office locations and contact information,
please visit imperva.com/contact-us

imperva.com