radware

Threat Report

2025 E-Commerce Bot Threat Report

Insights on malicious bots that disrupt online retailers—and destroy holiday sales.

Table of Contents

Executive Summary

The 2024 holiday shopping season recorded increasing sophistication in malicious bot activity targeting e-commerce platforms, with bad bots representing a consistently growing share of online shopping traffic. Online sales reached record volumes, while the corresponding surge in bot activity created significant security and operational challenges for digital retailers.

Our extensive analysis based on traffic to our e-commerce clients reveal that for the first time, **overall bot traffic eclipsed human user traffic during the 2024 holiday shopping season**, with malicious bot activity showing significant growth compared to previous years. Our analysis also indicates that bot operators are increasingly turning to sophisticated techniques to mimic human-like behavior, rendering many traditional detection methods ineffective.

The primary attack types identified in our analysis were price scraping, content scraping, account takeover attacks, fake account registrations, cart abandonments, and carding attacks, all with noticeably more sophistication in comparison to previous years. There is also a marked increase in bad bot attacks originating from traditionally trusted sources such as ISPs, the use of CAPTCHA farms to bypass security challenges, and a strategic shift toward targeting mobile platforms. These developments suggest that attackers are adapting in response to existing bot defensive measures while exploiting potential weaknesses in the e-commerce ecosystem.

According to Radware's 2025 Global Threat Analysis Report, overall bad bot transactions detected globally across industries in 2024 increased by 35% compared to the previous year, continuing the trend of rapidly increasing malicious bot traffic on online applications. Even more concerning is that 71% of bot traffic in 2024 was found to be comprised of bad bot activity, indicating the growing dominance of bad bots in overall bot traffic.

For security and business leaders, these findings underscore the critical importance of implementing advanced bot management solutions that go beyond traditional security approaches. E-retailers that fail to adapt to these evolving threats risk significant business impact during the crucial holiday shopping season, including revenue loss, damaged brand reputation, and customer attrition.

This comprehensive research report examines the growing sophistication of bot threats that target the critical holiday shopping period around Black Friday, providing actionable intelligence based on real-world attack data gathered during the 2024 holiday shopping season.

Key Findings

- **Overall bot traffic**, including both good bots and malicious bots, constituted 57% of total e-commerce website traffic during the holiday shopping period, increasing from the 49% recorded the previous year. This volume excludes bot-generated DDoS traffic, which otherwise would have considerably increased the recorded overall bot percentage.

  Click here to read more.

- **Bad bot traffic** demonstrated consistent growth, with more than half of detected bot traffic consisting of malicious bot activity during the 2024 holiday shopping season, compared to an equal share with good bots during the previous (2023) season. This growth is again without considering bot-generated DDoS traffic, which has grown considerably every year.

  Click here to learn more.

- A substantial portion of malicious bot traffic employed **sophisticated behavioral techniques to evade detection**, requiring advanced behavioral-based algorithms for detection, beyond just traditional signature-based techniques.

  Click here to learn more.

- **Distributed attack patterns** saw a marked increase, with attackers leveraging a wider network to evade rate-limiting, geo-based, and IP-based blocking mechanisms.

  Click here to learn more.

- **Malicious traffic originating from ISPs** notably increased, with bad bots attempting to mask their activity within traditionally legitimate network sources.

  Click here to learn more.

- **Heightened CAPTCHA farm activity** observed around the crucial sales days of Black Friday and Cyber Monday indicate attempts by attackers to bypass traditional CAPTCHA-based challenges.

  Click here to learn more.

- **Mobile-based bad bot attacks** more than doubled when compared to the previous year, indicating the shifting focus of attackers to target less-protected mobile platforms.

  Click here to learn more.

Overview

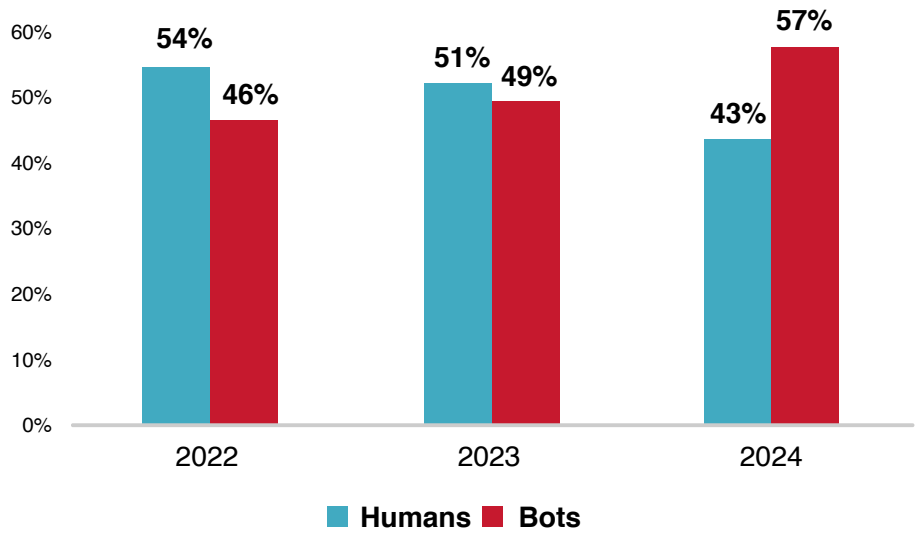
The annual shopping events surrounding Black Friday and the holiday season represent the most critical revenue-generating period of the year for e-commerce retailers. However, this concentration of consumer activity and financial transactions also offers a high-value target for malicious actors seeking to exploit the increased traffic and potential security vulnerabilities for unauthorized competitive intelligence gathering, fraudulent account takeovers etc.

Our analysis of traffic data on e-commerce platforms protected by Radware Bot Manager during the 2024 holiday shopping season revealed some dramatic shifts in bot traffic patterns that should be of concern to security and business leaders.

Overall bot traffic, including both good and bad bots, constituted approximately 57% of all e-commerce website traffic during the 2024 holiday shopping season, representing a 16% increase relative to the previous year. This meant that for the first time, e-commerce platforms received more automated bots than human shoppers during the crucial holiday shopping period, reflecting the growing dominance of automated traffic within the ecommerce ecosystem.

Figure 1:

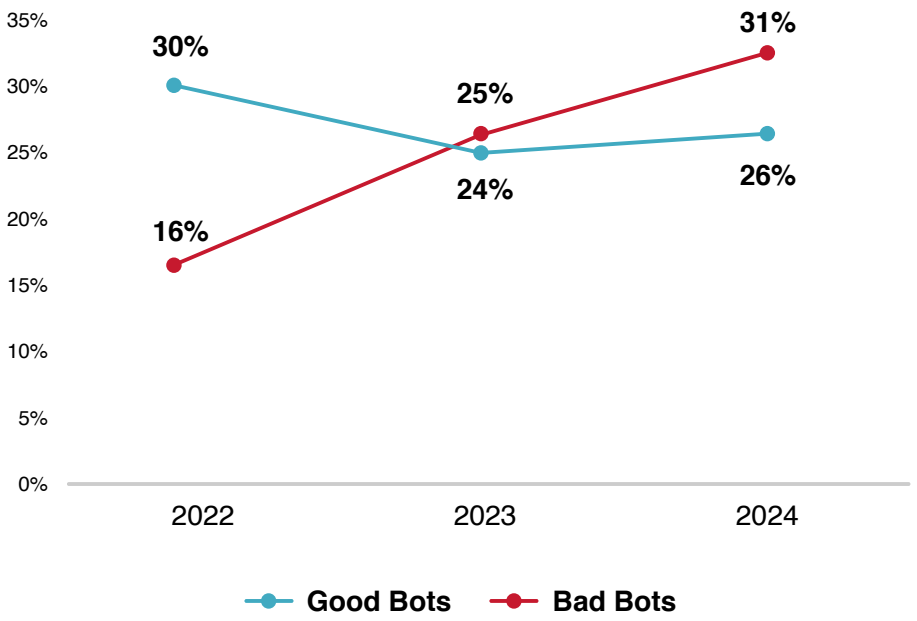
Share of human shopping traffic vs. overall bot traffic during the 2024 holiday shopping season



While some of this automated traffic came from legitimate sources like search engine crawlers and price aggregators, our analysis indicates that the share of malicious bots grew at a rapid pace over the years to account for approximately 31% of total shopping traffic in 2024, doubling from the 16% recorded just 2 years back—a worrying trend that directly impacts e-retailers' bottom lines and the customer experience during the crucial shopping season.

Figure 2:

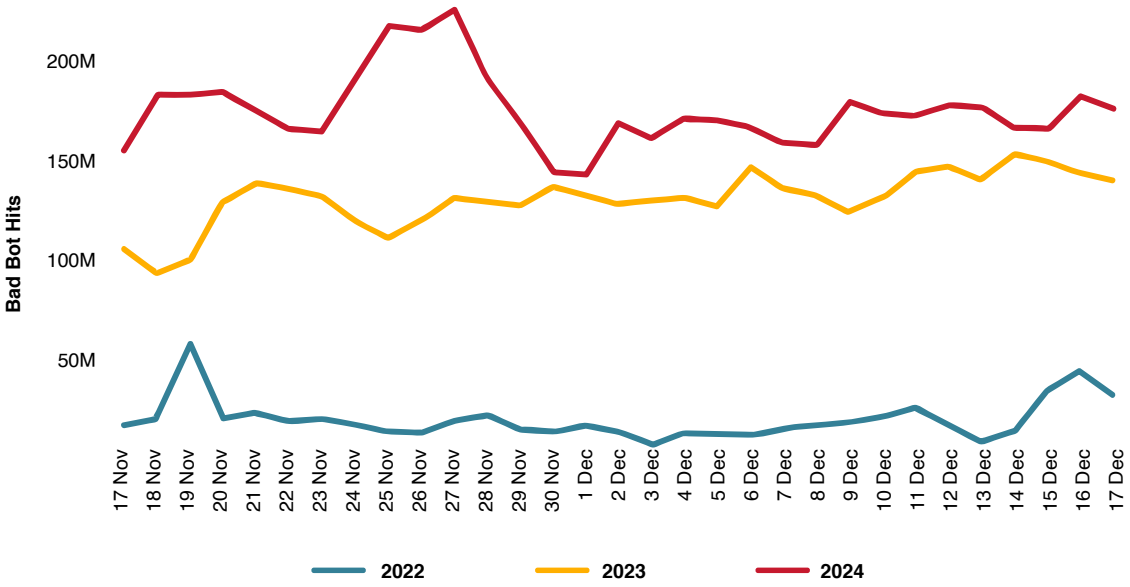
Trend of good bots vs. bad bot traffic during the 2022-2024 holiday shopping seasons



To put these numbers in perspective, the graph below shows the volume of bad bot traffic detected at a major multinational e-commerce website during the holiday shopping period over the years. The average volume of bad bot traffic detected on this client's platform during the period around Black Friday 2024 was over five times that of bad bot traffic in 2022. A key reason for this massive surge in malicious bot traffic could be attributed to the rapid advancements made in AI technology and development tools, with the easy availability of generative AI tools for bad bot development contributing to the significant increase in traffic from 2023.

Figure 3:

Bad bot traffic volume from 2022-2024 at a major multinational e-commerce website using Radware Bot Manager

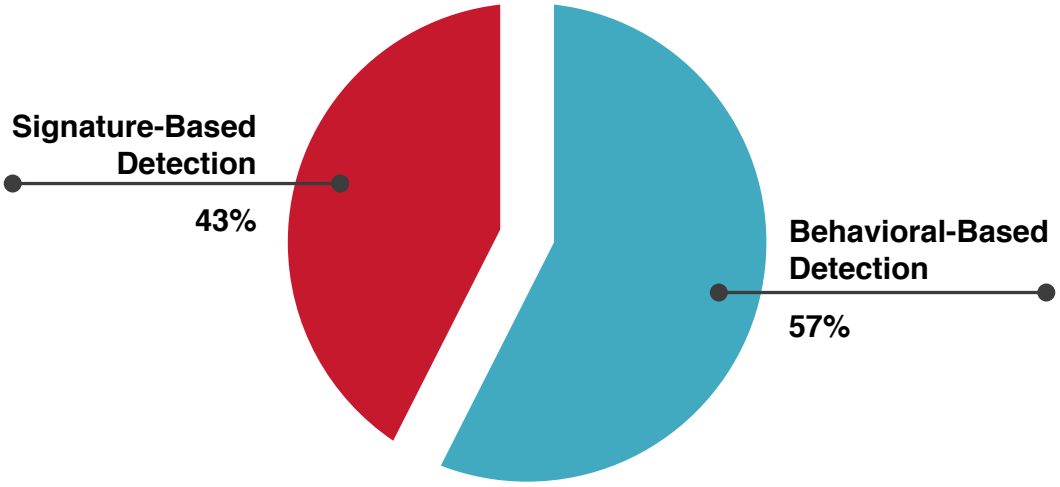


The Rise of Sophisticated Bot Attacks

One of the most notable insights observed during the 2024 holiday shopping season was the significant share of sophisticated behavioral-based bot attacks in the overall attack traffic. While signature-based attacks rely on predictable indicators that can be identified and blocked through traditional rule-based bot management solutions, behavioral-based attacks are designed to mimic human-like interaction patterns and browsing behaviors, making them substantially more difficult to detect.

Figure 4:

Proportion of malicious bots detected through signature-based vs. behavioral-based techniques

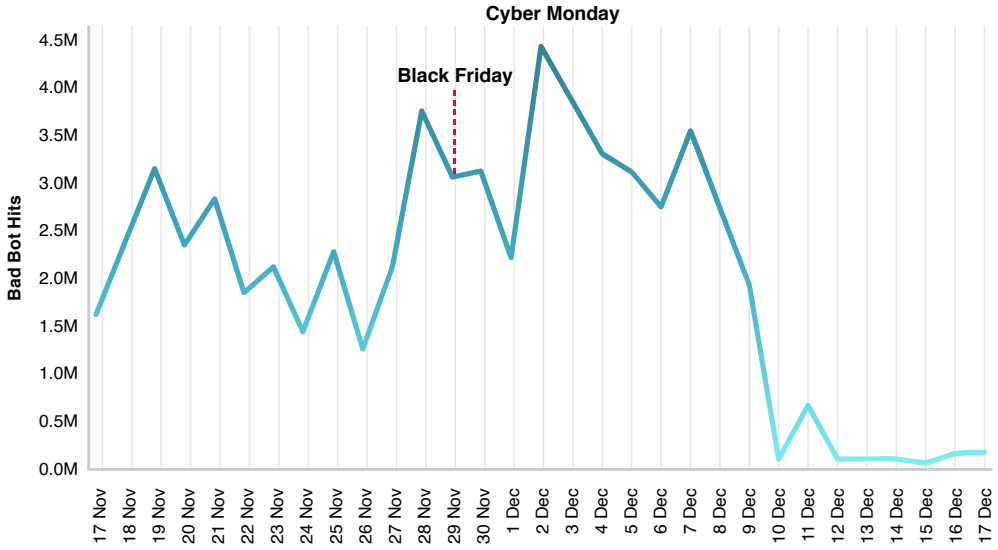


Our data indicates that 57% of malicious bot traffic detected during the 2024 holiday shopping period employed advanced behavioral techniques. These sophisticated bots demonstrate human-like behaviors including natural mouse movement patterns, click data behavior, and contextual website navigation similar to typical human shopping patterns.

This evolution towards human-like bot behavior in attacks requires more advanced detection methodologies that incorporate AI, machine learning, and behavioral-based algorithms to accurately distinguish between legitimate users and malicious bots.

Figure 5:

Trend of CAPTCHA farm activity detected on a client's e-commerce portal

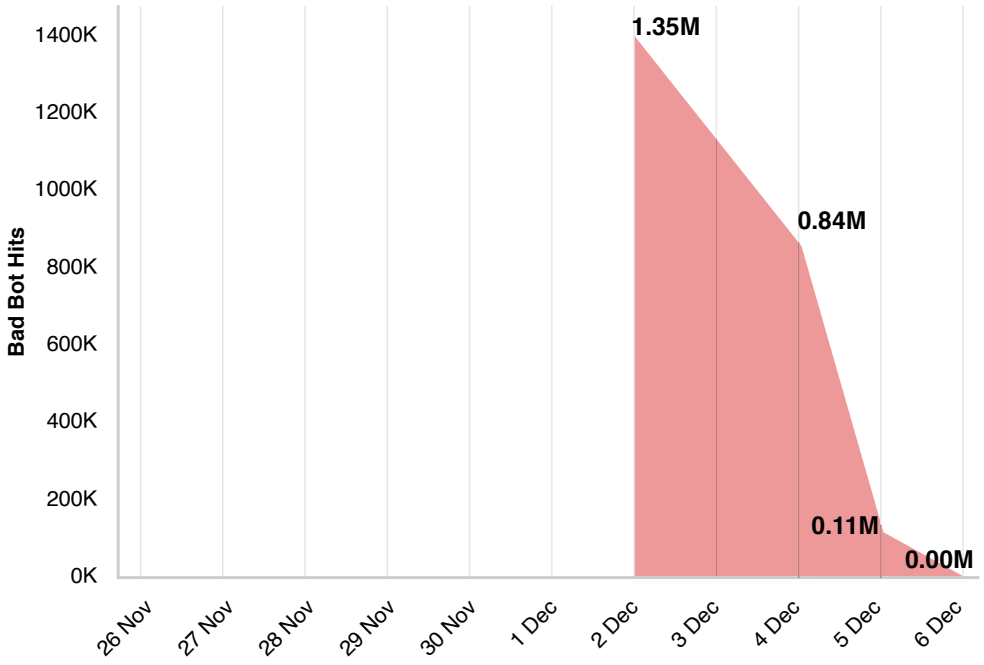


Our analysis also observed heightened activity from CAPTCHA farms—operations that employ third-party services to solve CAPTCHA security challenges—with noticeable surges detected and blocked during the crucial Black Friday and Cyber Monday sales periods, as seen in the graph above. The strategic timing of this increased activity suggests that attackers specifically scaled their operations around these high-value sales days, when a potential return on investment for CAPTCHA farm services could be maximized.

E-Commerce organizations that rely heavily on CAPTCHA mechanisms without additional security measures may find themselves increasingly vulnerable to such sophisticated bot operations that can effectively bypass this traditional protection layer.

Figure 6:

Sophisticated, distributed attacks detected at a client's website during Cyber Monday 2024 sales



A marked increase in distributed attacks was also observed, as represented with this particular example of an attack detected on our client during their Cyber Monday sales event. Rather than launching high-volume attacks from few available sources—an approach that makes detection relatively straightforward—attackers increasingly distribute their attacks across a larger, more diverse network of devices and IP addresses.

This evolution towards more distributed attack methodologies necessitates a corresponding evolution in defense strategies, with a shift away from simple IP reputation checks, blocking, and rate limiting, to more sophisticated approaches that can identify coordinated behavior across traffic sources.

The Shifting Focus of Attackers

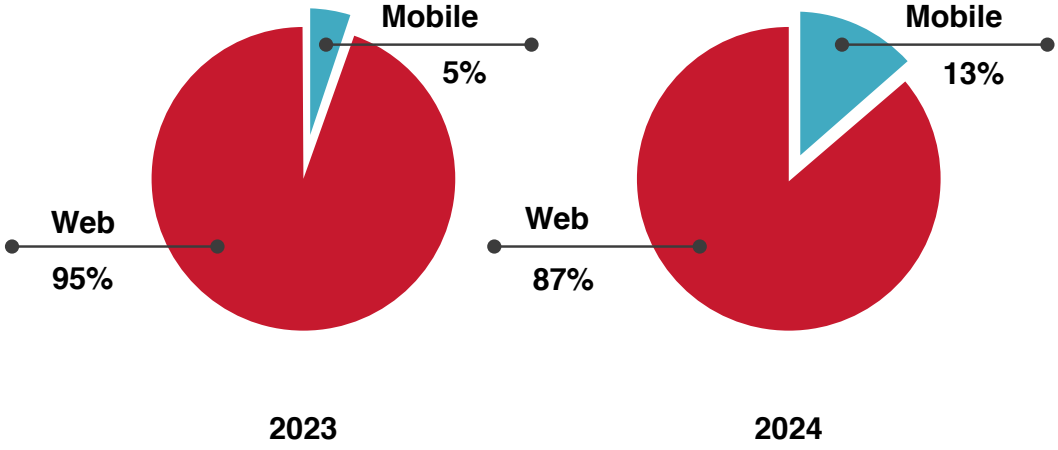
The 2024 holiday shopping season revealed significant shifts in attacker strategies, with two notable trends emerging from our analysis: a dramatic increase in attacks targeting mobile platforms, and a strategic shift towards leveraging ISP networks for malicious activities.

Increased Targeting of Mobile Platforms

Our data indicates that malicious bot traffic directed at mobile platforms increased by 160% when compared to 2023, representing a fundamental shift in attackers' focus.

Figure 7:

Split of bot traffic detected on web applications vs. mobile platforms across clients (2023 vs. 2024)



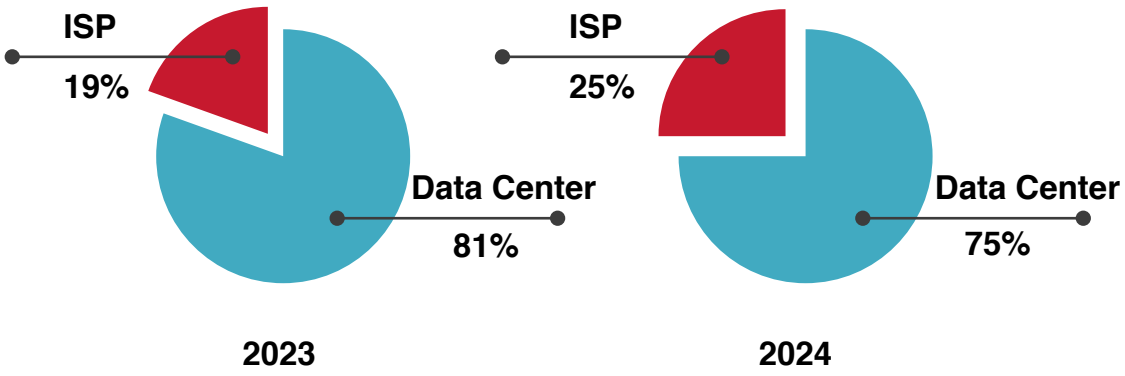
This shift appears to be driven by growing adoption of shopping on mobile applications and mobile-based transactions by consumers, combined with attackers recognizing the less robust security measures enforced on mobile platforms. The sharp uptick in malicious mobile-based traffic also suggests that attackers are leveraging more sophisticated techniques to target mobile users, including mobile emulators, mobile-specific proxies, and headless browsers with mobile user-agent strings, to effectively mimic user behavior.

This trend is particularly concerning given that many organizations focus their bot protection efforts primarily on web applications, potentially leaving mobile platforms completely vulnerable. The surge in mobile-targeted attacks suggest that attackers have identified this potential security gap, and are actively attempting to exploit it to increase their chances of success.

Figure 8:

Split of bad bot traffic originating from ISPs vs. data centers across our client base (2023 vs. 2024)

Growth in Bad Bot Traffic Originating from ISPs



The second notable shift identified in our analysis was the significant increase in malicious bot traffic originating from ISP networks including residential ISPs during the 2024 holiday shopping season. Historically, a substantial majority of malicious bot traffic originated from data centers, which offered more resources and capacity for large-scale attacks, but could also be more easily identified and blocked based on their source characteristics. However, our data indicates that the proportion of attack traffic originating from ISP networks increased by 32% during the 2024 holiday shopping season compared to the previous year.

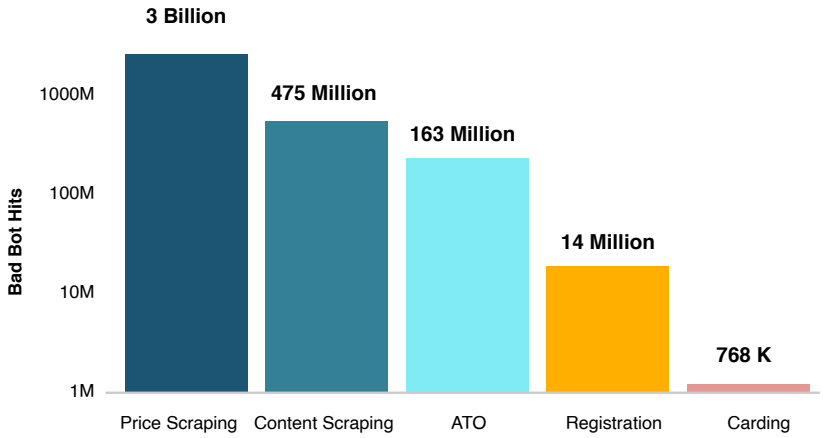
This growing shift of malicious bot traffic origin serves significant challenges for security teams, as ISP networks have traditionally been considered more legitimate or trusted compared to data center IP ranges. The growing availability of residential proxy services that provide attackers access to large pools of legitimate residential IP addresses could be one of the key factors driving this strategic shift. This makes it much harder for security teams to identify and stop the attack, since these services are used to mask the origin and make it appear as though the traffic is coming from genuine residential users. Traditional bot management approaches that rely on traffic origin in risk scoring may require adjustments to account for this evolution in attacker methodology.

Primary Bot Attack Types

Our analysis of client traffic data during the 2024 holiday shopping season indicates that price scraping operations continue to deploy the largest number of bots, causing a huge burden on e-commerce operations during major sales events. Yet, other types of attacks with comparatively lower volumes of bots detected can be just as damaging to e-retailers, if not more.

Figure 9:

Major types of bot attacks detected at a large multi-national e-commerce operator



In the above representation of attack traffic classification at a major multinational e-commerce firm protected by Radware Bot Manager, we observed that over 3 billion price scraping attacks were detected and blocked over the course of a 30-day period during the holiday shopping season. Content scraping was the next biggest attack type, with 475 million instances detected during the same period. Account Takeover attacks constituted 163 million attack detections, followed by fake account registrations, carding attempts, and other types of attacks.

The following sections examine the major types of bot attacks with examples of real-world incidents from the holiday shopping season, describing the attack mechanisms, our analysis of attack data, and details of their impact on e-retail businesses.

Price Scraping

"3x more price scraping attempts detected on Black Friday"

Attack Mechanism

Price scraping attacks involve the systematic extraction of product pricing information from e-commerce websites, typically conducted by competitors or third-party aggregators seeking to gain competitive intelligence or inform their own pricing strategies. Around Black Friday in particular and across the holiday shopping season in general, scraping activities by competitors or aggregators operate at a massive scale, particularly focused on monitoring flash sales, limited time offers, and dynamic pricing adjustments. Modern price scraping bots are highly sophisticated, capable of extracting large-scale pricing data while maintaining a low profile.

Holiday Traffic Data Observations

In the graph below that shows the trend of price scraping attacks detected at an e-commerce website protected by Radware Bot Manager, the highest concentration of scraping activity was observed on Black Friday with more than 3 times the volume of scraping attempts compared to other days.

Figure 10:

Trend of price scraping attack activity detected on a client's e-commerce website (11/17/2024 – 12/17/2024)

From our analysis, 112,000 price scraping instances were detected on 63,000 of this e-retailer's unique product pages on Black Friday. Over 1.2 million price scraping instances were recorded and blocked on the platform over a 30-day period during the sales season, representing the massive scale of attack traffic faced from just this attack type alone. The noticeable uptick in scraping activity on and around the crucial sales days indicates the strategic focus of malicious actors in monitoring competitive pricing during high-value promotional windows.

Business Impact

Competitive Disadvantage: Competitors leveraging scraped data gain significant intelligence into pricing strategies. Real-time visibility into pricing adjustments and promotions can effectively neutralize the competitive advantage of a retailer's pricing strategy.

Infrastructure Overload: High-volume scraping operations consume substantial system resources, impact site performance, and cause performance degradation that affects legitimate customer experiences.

Skewed Analytics: Price scraping bots can skew web analytics data by misrepresenting consumer interest or engagement in specific products or categories, and lead to misguided marketing decisions.

"5x spike in content scraping activity on the day before Black Friday"

Content Scraping

In the graph below that shows the trend of price scraping attacks detected at an e-commerce website protected by Radware Bot Manager, the highest concentration of scraping activity was observed on Black Friday with more than 3 times the volume of scraping attempts compared to other days.

Attack Mechanism

Content scraping attacks involve malicious bots systematically extracting e-retailers' proprietary information, including product descriptions, images, customer reviews, specifications, and other valuable content to pass off as their own. Modern content scraping bots enhanced with the latest technology can continuously monitor and extract diverse types of content from target websites. The scraped content is then repurposed on competing sites, damaging the original retailer's search engine rankings and value propositions.

Holiday Traffic Data Observations

From our analysis of traffic to a large e-commerce operator during the 2024 holiday shopping season, we observed a dramatic 5x spike in content scraping activity on the day immediately before Black Friday, with 58,000 bad bot hits recorded on the platform's content pages. This most likely represents competitors or third-party entities rushing to extract the retailer's proprietary data including product descriptions, images, reviews, etc., before the sale period starts. On the same day, Bot Manager blocked scraping attempts on over 7,000 unique URLs and over 340 unique category pages that were targeted during the attack.

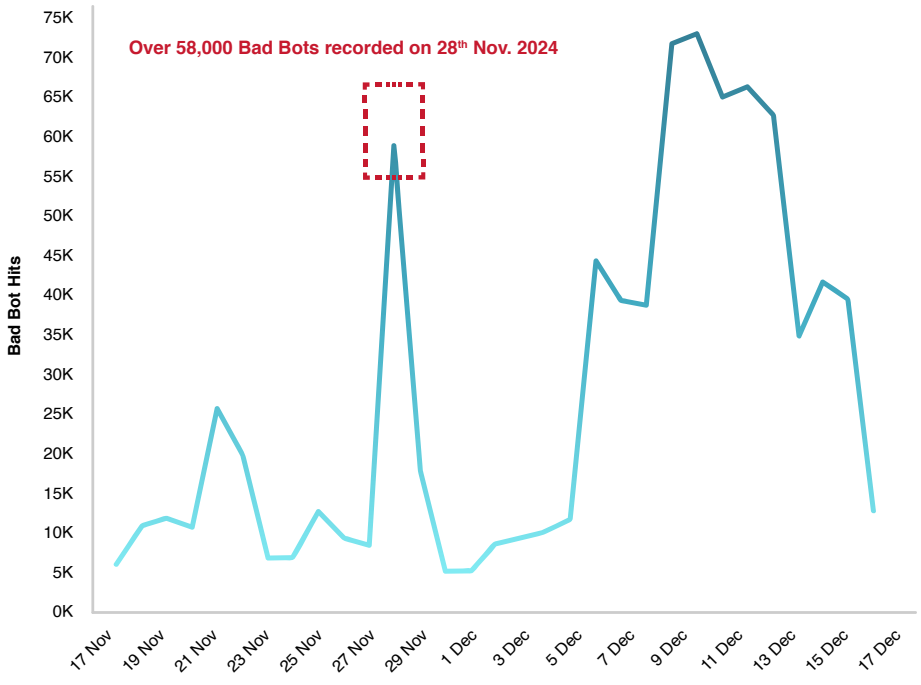


Figure 11:

Trend of content scraping activity detected at an e-commerce firm (11/17/2024 – 12/17/2024)

A sustained surge in content scraping attempts was also observed a few days after Black Friday, which could represent efforts by competitors to analyze changes to the e-retailer's content inventory post-Black Friday, including updated customer reviews, revised marketing messaging, and other information in preparation for the extended holiday shopping season.

Business Impact

Competitive Disadvantage: Many e-retailers heavily invest in unique product descriptions, high-quality photography, detailed specifications, and other supporting content. Systematic extraction of this content by competitors reduces the competitive advantage they provide, potentially diverting customers and sales.

SEO Damage: Search engines may penalize the original retailer for duplicate content if the copied content is available on other websites, lowering their search rankings and reducing organic traffic.

Reduced Customer Trust: When customers encounter identical content across multiple e-commerce platforms, it can create confusion about product authenticity and undermine confidence in the original retailer.

"3x more ATO attempts detected on the day before Black Friday"

Account Takeover

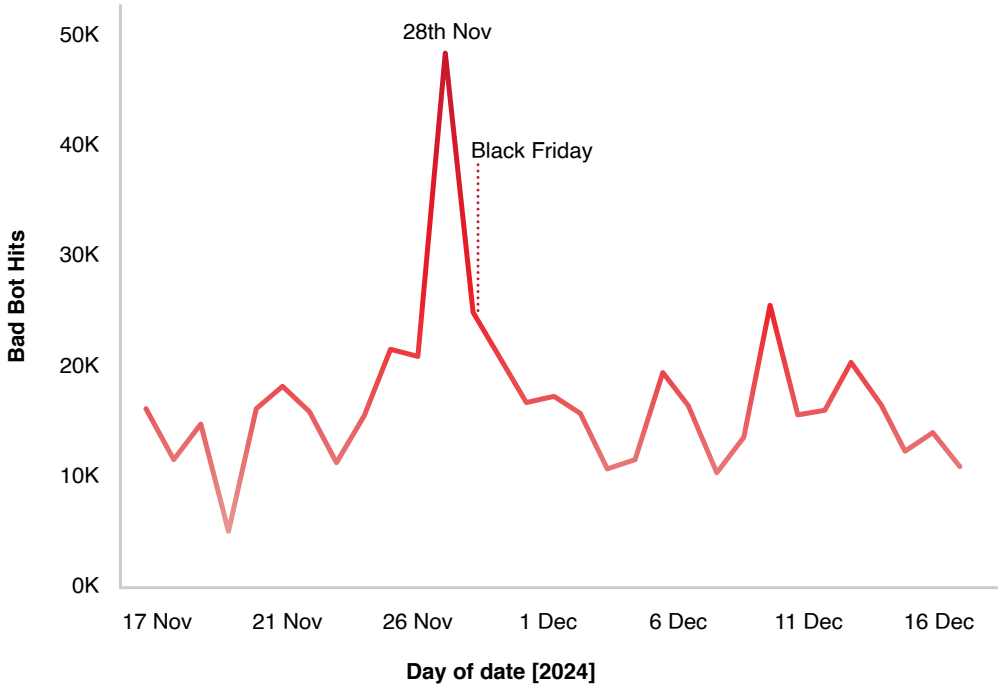
Attack Mechanism

Account takeover (ATO) attacks involve malicious actors gaining unauthorized access to customer accounts through credential stuffing, credential cracking, or brute force methods. In the period leading up to Black Friday, attackers collect vast databases of stolen credentials from data breaches and dark web sources. When shopping activity intensifies around key sales days, sophisticated bots are deployed to brute-force into account login workflows, attempting to blend in with the high volume of traffic and looking to gain access to stored payment information, personal data, and other personally identifiable information.

Holiday Traffic Data Observations

Figure 12:

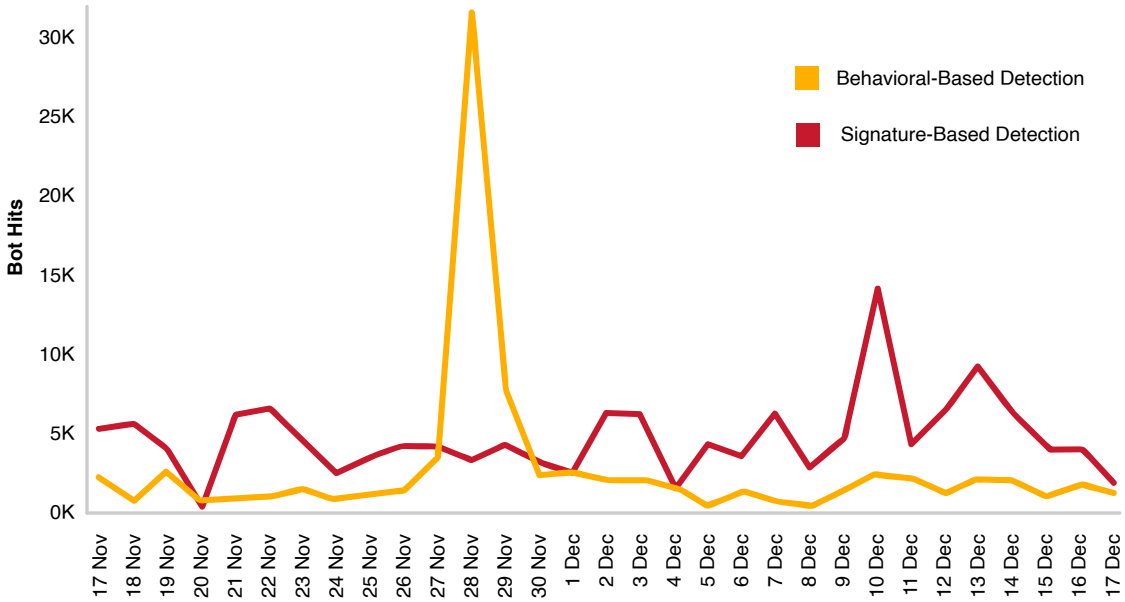
Trend of account takeover attacks detected on a client's e-commerce website



From traffic data at a major e-commerce platform protected by Radware Bot Manager, we observed 3x the ATO attempts detected on the day before Black Friday sales, at ~50,000 bot hits on their login workflow, compared to regular days. Customer account activity was at its peak just before the sales events began, when they often add their payment information, load their digital wallets, and update their personal information in preparation for their purchases. This is ideal for attackers looking to increase their chances of gaining the most value from their efforts. Over 500,000 ATO attempts were detected on the login pages of this client's platform over this key 30-day sales period.

Figure 13:

Trend of ATO attacks detected with behavioral-based detection vs. signature-based detection (on the same platform)



A very significant observation from the attack data on this website was the substantial share of malicious bots emulating sophisticated human-like behavioral traits in their attack operations. From our analysis, 60% of the bot hits on the day of peak ATO activity were detected using our advanced behavioral-based detection algorithms, as seen in the graph above. This indicates that attackers were deploying their most advanced bots during the most lucrative period of customer activity, and distributing the less-sophisticated attacks throughout the rest of the shopping season.

Business Impact

Financial Losses: While direct fraudulent transactions from customer accounts represent the most visible cost of ATO attacks, they often account for only a portion of the total financial impact. The resulting chargeback claims, refunds, lawsuits, investigation costs, account remediation costs, etc. typically constitute a major portion of the losses.

Increased Operational Overhead: Account takeover incidents lead to an increase in customer complaints and generate significant customer service requirements, particularly during the already high-volume holiday period, creating substantial additional operational costs.

Customer Trust & Reputation Damage: Breaches of sensitive customer data significantly damage brand reputation and customer loyalty, particularly when they involve stored payment information or personal data. With the potential for negative publicity that can quickly spread through social media channels, the reputational damage can extend beyond customers to influence broader market perception.

Regulatory Exposure: Account takeovers and subsequent data breaches often trigger various regulatory reporting requirements and lead to regulatory scrutiny with financial penalties, under data protection regulations such as the GDPR, CPRA, NIS2, and others.

"Spike in fake account registrations 2 days before Black Friday with sustained surge throughout"

Fake Account Registrations

Attack Mechanism

Account takeover (ATO) attacks involve malicious actors gaining unauthorized access to customer accounts through credential stuffing, credential cracking, or brute force methods. In the period leading up to Black Friday, attackers collect vast databases of stolen credentials from data breaches and dark web sources. When shopping activity intensifies around key sales days, sophisticated bots are deployed to brute-force into account login workflows, attempting to blend in with the high volume of traffic and looking to gain access to stored payment information, personal data, and other personally identifiable information.

Holiday Traffic Data Observations

From attack data recorded at one of our large, multi-national e-commerce clients, we observed a spike in fake account creation attempts two days before the Black Friday sales event, with another spike detected closer to sales events around Christmas.

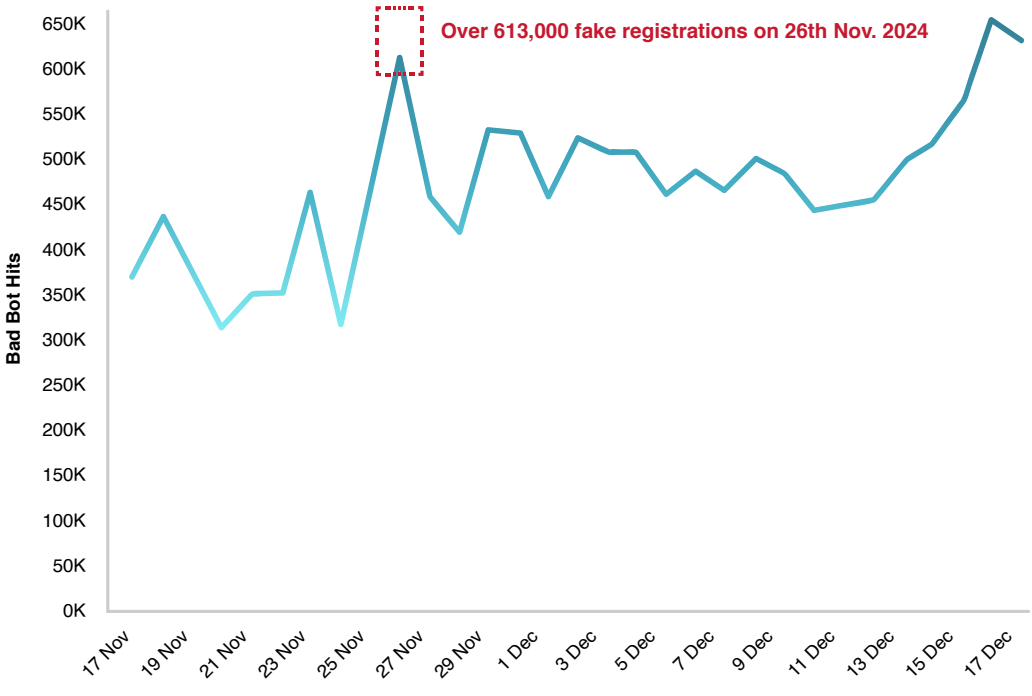


Figure 14:

Trend of fake registration attacks detected at a client's e-commerce portal

Over 613,000 fake registration attempts were recorded on 26th November, 2024, as attackers moved in to create fake user accounts before Black Friday and capitalize on sales day promotions and offers. A sustained surge in these attacks was observed during the period around critical sales events with over 14 million fake registration attempts recorded during the 30-day period that included Black Friday and Cyber Monday. This highlights the growing inclination of attackers to allocate their resources to this attack vector, most probably based on prior success at other e-commerce platforms.

On 26th November, the fake registration bot hits recorded originated from over 200,000 unique IPs and user agents. The large number of unique IPs and user agents recorded with relatively consistent bad bot hits, suggests that the attacks are programmatically managed using a large-scale, distributed botnet or proxy network, and rotating IP addresses and/ or user agents through coordinated bot behavior. This evasive attack methodology makes it harder to mitigate through traditional mitigation techniques such as simple IP blocking or rate limiting.

Business Impact

Promotion Abuse: Fake accounts created around the peak shopping season are used to exploit new-customer discounts, referral programs, and other promotional offers devised by e-retailers to drive customer acquisition during the high-traffic holiday shopping season.

Distorted Business Metrics: Large volumes of fake accounts can significantly skew key business metrics including customer acquisition costs, conversion rates, and more. These distortions can lead to misguided marketing decisions based on inflated user numbers.

Increased Fraud Risk: Once created, fake accounts serve as foundations for various other fraudulent activities such as carding, promotion abuse, and spamming.

"Sharp spikes in cart abandonment activity on and around Black Friday"

Cart Abandonment

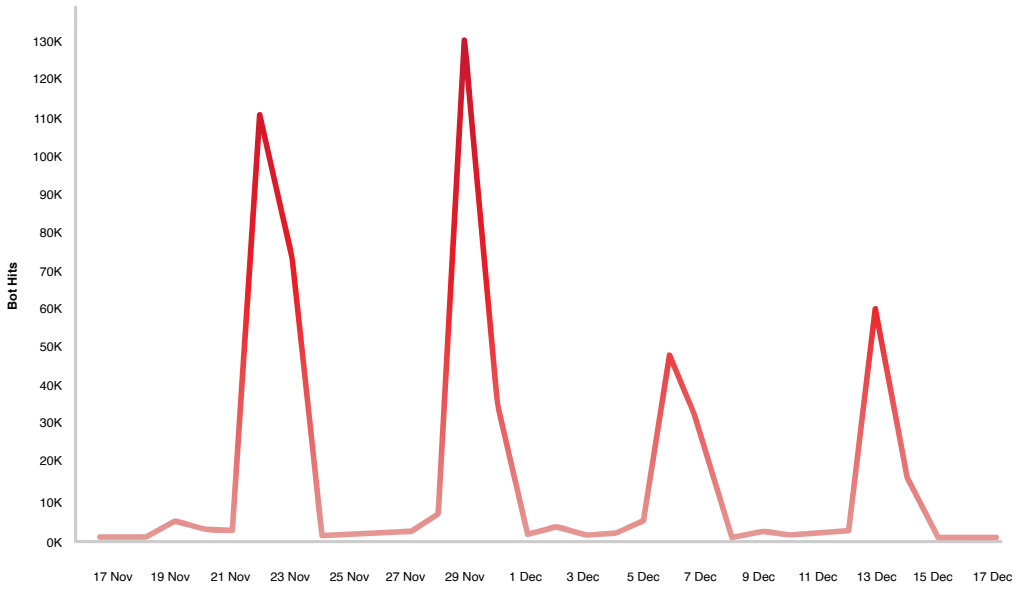
Attack Mechanism

Cart abandonment attacks—also referred to as denial of inventory—involve malicious bots automatically adding items to shopping carts, but without checking out and completing the purchase. During critical sales events, this is repeated at a massive scale, preventing genuine buyers from purchasing desired goods and leading to customer churn and lost sales. To counter this attack, most e-retailers have set time limits on how long items are reserved within shopping carts per user session. Modern bots, though, bypass this measure by revisiting the website after a preset duration.

Holiday Traffic Observations

Figure 15:

Trend of cart abandonment attacks observed at an online retail website (11/17/2024 – 12/17/2024)



From attack data recorded at a retail portal secured by Bot Manager, we observed sharp spikes in cart abandonments detected around the key sales days. The biggest spike in attacks with over 130,000 cart abandonments was recorded on Black Friday, with attackers strategically targeting the event, looking to maximize disruption and financial losses. These attacks are often distributed in nature, spread across thousands of IP addresses to evade traditional detection methods. Adding a high-demand or limited availability item to the cart with no intention of purchasing it can prevent genuine users from purchasing goods while also disrupting inventory management strategies.

Business Impact

Financial Losses: During key sales days, malicious bots can add items to carts much faster than genuine users. This artificial reduction in inventory renders the item unavailable, causing customers to churn, or purchase products from other retailers, in both cases leading to lost sales opportunities and financial losses.

Skewed Analytics: Cart abandonment rates and conversion rates are key metrics for e-retailers and especially so during the high-stakes holiday shopping season. Artificially inflated cart abandonments by malicious bots leads to inaccurate analytics, making it harder for businesses to gauge consumer behavior and can lead to misguided marketing decisions.

Inventory Management Disruption: Bots adding large quantities of products without purchasing them can cause false demand signals that disrupt inventory forecasting and management strategies, creating costly inefficiencies throughout the supply chain.

Poor User Experience: Genuine buyers being unable to purchase items due to stock unavailability during the crucial sales events can lead to a negative user experience. Potential customers landing on e-retail portals through targeted ads promoting product availability and discounts can move on and shop elsewhere, causing losses on marketing and inventory investments.

"768K carding attacks blocked over 30 days of shopping season"

Carding Attacks

Attack Mechanism

Carding attacks involve the systematic testing of stolen credit/debit card information on e-commerce payment workflows to verify its validity. Modern carding operations employ sophisticated techniques to navigate checkout processes while distributing their attacks across thousands of accounts and IP addresses to evade rate-based detection. Successfully validated payment card data are then used for larger fraudulent transactions on the same platform, other retailers, or even resold on the dark web for profit.

Holiday Traffic Observations

While the scale of carding attacks on e-retailers during the holiday shopping season may seem small compared to scraping attacks, it is important to remember that price and content scraping bots work in bulk across thousands of product pages and usually operate for an extended period to monitor the latest changes. Meanwhile carding attacks are focused only on the e-retailer's payment workflow, directly impacting critical payment pages, with each successful attack potentially causing exponential losses.

In the case of attack data observed in fig.9, if the 768,000 carding attacks detected over a 30-day period during the shopping season had gone unmitigated, the potential losses could range in the tens of millions of dollars, causing a devastating financial impact.

Business Impact

Increased Chargebacks and Related Costs: Successful carding attempts result in monetary losses from fraudulent transactions as well as chargebacks once cardholders identify the unauthorized transactions. Higher chargeback rates can trigger penalties from payment processors, while the additional operational expenses for incident response, investigation, and customer support can quickly add up.

Loss of Customer Trust: Customers who experience unauthorized financial transactions can lose confidence in the e-retailer's security measures, leading to damaged brand reputation and credibility.

Regulatory Penalties: Failure to protect customer payment data and prevent potential fraud can result in hefty fines and penalties if they are found in breach of regulations such as PCI DSS, GDPR, and NIS2, among others.

Emerging Threats for the 2025 Holiday Shopping Season

From our analysis of bad bot traffic trends during the 2024 holiday shopping season, several emerging threat vectors become apparent that are likely to present significant challenges for e-retailers' security teams in the upcoming holiday season.

The Advancement of AI-Enhanced Bots

The most significant emerging threat is the continued advancement of AI-enhanced bot capabilities. The widespread availability of generative AI technology is lowering the barrier to entry for new cybercriminals and democratizing bot development due to the ease of scripting them using basic prompts. This is not just limited to attacks on e-commerce, and is evident from the 35% increase in overall bad bot transactions detected across industries in 2024 compared to the previous year.

Generative AI is enabling experienced attackers to develop more sophisticated bots that display increasingly human-like behaviors, navigate complex web interactions, and evade traditional detection methods. AI tools are also accelerating bot development lifecycles by enabling the rapid creation, iteration, debugging, and retooling of new bot variants, leading to more persistent and aggressive attack campaigns.

AI capabilities that could further drive this shift are:

- Natural language processing and other automation tools that enable bad bots to generate and fill user information to create fake accounts, simulate online engagement, or submit spam with a malicious intent.
- Optical Character Recognition (OCR), advanced AI algorithms, and machine learning capabilities to bypass advanced audio-based or image-based CAPTCHA challenges.
- Adaptive decision-making capabilities that enable bad bots to adjust strategies in real-time based on encountered security measures.
- Development of agentic AI-driven bots based on large language models (LLMs) requiring limited human supervision to interact with other environments and perform attacks.

Mobile-focused Attack Vectors

As mobile shopping continues to drive e-commerce growth, we anticipate a significant shift towards mobile-focused attack vectors during the upcoming holiday shopping season. This shift reflects both the increasing share of transactions occurring on mobile devices and the unique security challenges presented by mobile platforms. Native mobile applications rely heavily on APIs and lack browser-based interaction, rendering the traditional CAPTCHA-based or JavaScript validation-based challenges ineffective in malicious bot detection. We anticipate attackers looking to increasingly target these mobile-specific vulnerabilities and exploit security weaknesses in mobile applications.

Distributed Infrastructure Attacks

Attackers could continue to exploit distributed cloud infrastructure and residential proxy networks to execute attacks at unprecedented scale while evading detection and mitigation efforts. The easy availability of residential proxy services allows attackers to generate malicious traffic from what are usually considered to be safe, genuine sources. Along with a distributed approach and rotating through proxies, this creates significant challenges for traditional security measures that rely on IP reputation, usage patterns, and the like.

Multi-Vector Attack Strategies

Attackers employing coordinated multi-vector campaigns instead of single-approach attacks is a trend we've observed and anticipate growing in strength in the future. Rather than focusing only on bot attacks, attackers are targeting applications through a combination of bot attacks, web application vulnerability exploits, business logic attacks, and API-focused attacks. This diversified approach allows attackers to maximize their chances of success by probing different defensive layers that protect applications. It also complicates defensive measures by retailers' security teams that are already burdened with high traffic volume during the holiday shopping season.

Radware's Recommendations for E-Commerce Organizations

Implement Advanced, Multi-Layered Bot Management

The increasing sophistication of bot attacks requires a comprehensive defensive approach that combines advanced detection and mitigation capabilities. Key components of an effective multi-layered bot management solution include:

- **Preemptive Protection:** Proactively detecting and blocking known malicious identities based on latest threat intelligence on the evolving threat landscape, with cross-correlation of security threats across other application security modules. The objective should be to stop bot attacks before they even materialize and take a toll on internal infrastructure.
- **AI-powered Bot Detection:** Employing AI-powered, behavioral-based algorithms capable of identifying, in real-time, anomalous behavior from even the most sophisticated human-like bots. The solution should be capable of accurately distinguishing between humans and sophisticated bots that utilize attack patterns including rotating IPs and identities, distributed attacks, CAPTCHA-solving services, and other advanced anomalies, without causing false positives.
- **Advanced Granular Mitigation:** Deploying real-time mitigation signatures that effectively stop malicious bots while minimizing friction for legitimate users. The solution should offer a wide range of mitigation challenges including fully non-interactive options that can be deployed based on the risk level and severity of the bot attack without affecting the user experience.

Develop Mobile-Specific Security Strategies

Given the considerable increase in mobile-targeted bot attacks observed during the 2024 holiday shopping season, organizations must develop security strategies tailored to mobile platforms. Dedicated mobile bot management SDKs within native mobile applications can provide enhanced visibility into interaction patterns and mobile-focused attacks that may not be observable through traditional web security approaches. The solution should be capable of defending against mobile emulators and maliciously modified applications (as well as similar obfuscatory tactics), to ensure that only genuine devices get access to resources.

Adopt an Integrated Application Security Strategy

With attackers increasingly deploying multi-vector attack campaigns that target multiple defensive layers of applications, it is imperative for retailers to adopt an integrated application security strategy that can leverage the latest threat intelligence and cross-correlate security threats across security modules. This holistic approach to application security ensures end-to-end visibility for security teams, allowing a coordinated defense to a wide variety of threats, and enabling consistent application of security policies across modules including bot management, WAF, API security, DDoS Protection, client-side protection, and other protective measures.

Onboard Managed Security Services

Onboarding an expert team of security professionals who offer specialized protection services can elevate an e-retailer's application protection strategy. The proactive support, extensive threat intelligence, experienced skillsets, 24/7 monitoring, and rapid attack resolution offered by such a team can help internal security teams share responsibilities to ensure comprehensive protection and avoid application downtime during the critical holiday shopping season and throughout the year.

Conclusion

The 2024 holiday shopping season revealed both the continuing evolution of established bot threats and the emergence of more sophisticated attack methodologies targeting e-commerce platforms. The trends observed—including the large share of behavioral emulation attacks, the increasing focus on mobile platforms, more evasive distributed attack techniques, and the growing sophistication of attack tactics—indicate a strategic shift in how malicious attackers approach the high-stakes holiday shopping season.

It is evident that attackers are specifically targeting key sales events to launch sophisticated bot attacks that exploit the increased traffic volumes, promotional activities, and operational overheads that characterize this critical shopping period. This strategic targeting requires equally strategic defensive approaches that recognize the evolving sophistication of the bot threat landscape, instead of relying on traditional, signature-based bot defense mechanisms.

E-commerce organizations must recognize that bot management is not simply a technical challenge but a fundamental business imperative that directly impacts competitive positioning, customer experience, and financial performance during the important holiday shopping period. Organizations that adopt a proactive security posture will be best positioned to protect their customers, operations, and bottom lines during future holiday shopping seasons.

Key Takeaways:

- The highest-ever volume of bad bot traffic was detected on e-commerce platforms during the 2024 holiday shopping season.
- The majority of malicious bots detected employed sophisticated human-like behavior to evade traditional, signature-based detection.
- Attackers are shifting focus towards more vulnerable mobile platforms, native mobile apps, and blending in with safer, ISP-origin traffic.
- Price scraping attacks were highest by volume, but other attack types such as account takeover and fake registrations still pose higher-than-ever security risks and business impact.
- Advanced, multi-layered bot management is more important than ever to defend against modern attackers armed with sophisticated, AI-enhanced bots.
- Distributed, multi-vector attack trends are on the rise, requiring a proactive, integrated application protection strategy supported by expert managed services.

For a broader analysis of the Global Network and Application Attack Trends in 2024 across industries based on Radware Threat Intelligence, please read our 2025 Global Threat Analysis Report.

How secure is your website against malicious bot attacks? Use our free vulnerability scanner to find out now.

Radware Application Vulnerability Scanner

RWI 499 | 04.17.2025