2022 Automated Fraud Benchmark Report

An inside look at the automated attack trends impacting e-commerce retailers

HUMAN

2022 Automated Fraud Benchmark Report

Table of Contents

The Significance of the E-commerce Account

Digital engagement has skyrocketed in recent years, which means an evolution in the way consumers interact with e-commerce web and mobile apps. It is easier than ever to discover new brands, buy desired products and make accounts to store personal and payment information for a seamless shopping experience.

With the digital surge, more consumers are storing more personal information and payment data in their online retail accounts. This includes stored credit cards, gift card balances, loyalty points and personally identifiable information (PII). Accounts are a treasure trove of value, which makes e-commerce apps the perfect target for automated attacks.

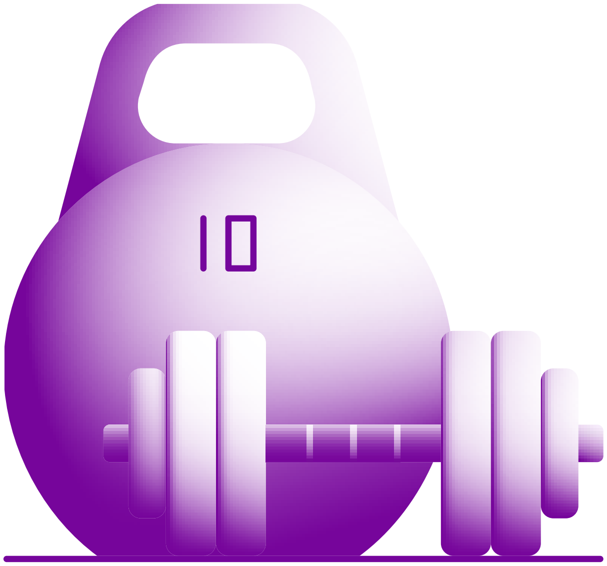
But even more significant is that accounts now hold a piece of a user's identity — and that's much more valuable than a stored credit card. If a cybercriminal can hide behind a legitimate user's identity, the opportunities to commit fraud increase significantly. And when it comes to protecting consumers' identity, your reputation and revenue are on the line.

1.

Executive Summary

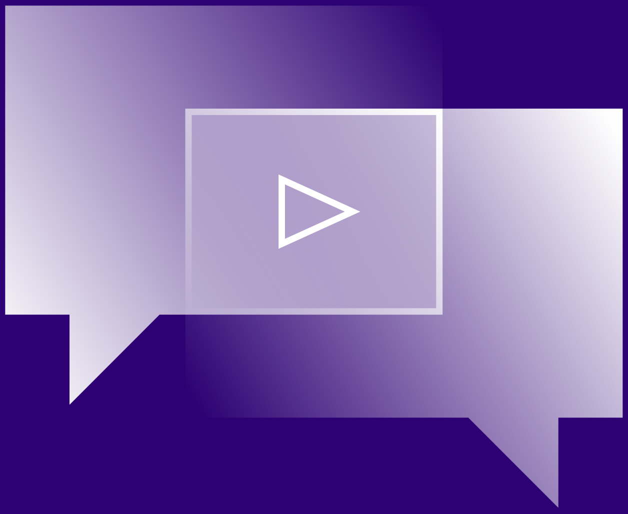
The annual HUMAN Automated Fraud Benchmark Report provides insights into automated attack trends gathered from billions of online interactions across hundreds of the world's largest shopping sites. Here are the key takeaways:

- Total traffic to e-commerce sites fell 3.38% in 2021
- Bot attacks increased 106.21% YoY in 2021
- Carding attacks increased 111.61% YoY in 2021.
- Peak malicious login attempts increased 9.13%, from 84.71% in 2020 to 93.84% in 2021.
- Scraping attacks rose 240% YoY.
- The three segments that saw the most bad bot traffic were Health and Wellness (36.28%); Hardware, Software and Electronics (33.2%); and Sports and Recreation (27.9%).
- Sales of limited-edition sneakers specifically experienced up to 71.61% traffic from scalping bots during hype sales events in 2021, an increase from the 2020 peak of 46.87%.
- Roughly three-fourths (74.7%) of malicious requests came from desktop device user-agents and the remainder from mobile device user-agents.
- 71.88% of total traffic from the Åland Islands, an autonomous region of Finland, came from bad bots; this was the highest of any region.



2. Methodology

→ The information in this report represents bot traffic across thousands of applications, infrastructure elements and endpoint devices in 2021. The data was pulled from sensors integrated into the front end, middleware and web servers of hundreds of e-commerce platforms, applications and content delivery networks (CDNs). Researchers used an out-of-band process, so there was no impact on the performance of monitored traffic or applications. The data was anonymized to preserve privacy, and any confidential company data was removed. HUMAN did not collect any personally identifiable information (PII) for this report. Note that the data in this report has been normalized; the bottom 25% of outliers have been removed so as to not skew the results.



3. Attack Definitions

Scraping

→ Bots crawl websites to capture pricing information, product descriptions, inventory data or copyrighted content and images. Competitors use the information to gain a competitive advantage. Furthermore, if search engines detect duplicate content, it can damage the original site's SEO rank.

Credential Stuffing

→ Fraudsters use bots to attempt logins on e-commerce sites with stolen usernames and passwords. If a login is successful, the validated credential pair is used by the cybercriminals to commit future online fraud or sold on the dark web.

Account Takeover (ATO)

→ ATO attacks, also called account fraud, occur when cybercriminals take unauthorized ownership of online accounts using stolen credentials. This allows them to make fraudulent purchases with stored payment data; steal gift cards and loyalty points; write fake reviews; submit fake warranty claims and create fake accounts. .

Digital Skimming and PII Harvesting

→ Cybercriminals exploit security weaknesses in website code to inject malicious scripts that skim users' payment data and other PII. While these are not types of bot attacks, the stolen PII is used in credential stuffing, carding and account takeover attacks.

Carding

→ Attackers use bots to test stolen credit card and debit card data by making small purchases on e-commerce sites. Validated cards are used to make subsequent fraudulent purchases of products or gift cards, which are then converted into high-value goods and resold online. Gift card cracking is a type of carding where cybercriminals validate gift card numbers in a brute force attack.

Scalping

→ Automated bots buy coveted products, such as limited-edition sneakers, gaming consoles, collectible cards and coins, concert tickets or hot toys. The high-demand items are later sold at inflated prices on third-party sites or the dark web.

4.

Overall Traffic

The start of the pandemic in 2020 marked the start of an unprecedented surge in web traffic to e-commerce sites. As more people began to store value in online retail accounts, cybercriminals seized the opportunity to reap even bigger rewards from their attacks.

Web traffic fell 3.38% on average in 2021. Although traffic in March 2021 surpassed the initial pandemic surge, it declined sharply thereafter. Traffic rose again during the 2021 holiday season, but it never again reached its 2020 height.

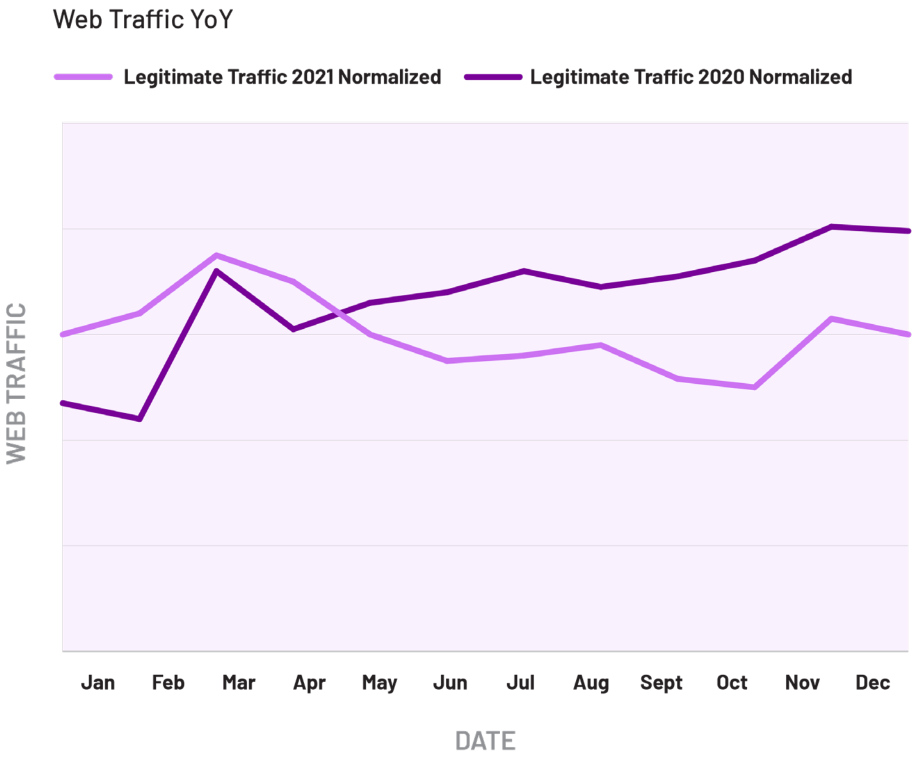


Figure 1: Legitimate web traffic in 2020 and 2021

Bad Bot Traffic

→ Despite the decrease in traffic to e-commerce sites in 2021, the percentage of malicious bot traffic remained the same. The average percentage of malicious bot traffic in 2020 was 29.5%, while the average in 2021 was 29.4%. This indicates that cybercriminals aren't slowing down just because consumers are spending more time offline. In fact, malicious traffic was up 106.21% in terms of total normalized requests.

Today's online retailers collect more personal and payment data than ever before, and it's all held inside consumer accounts. Even as social distancing regulations have become more relaxed and people have once again begun to shop in-store, their online accounts remain intact — meaning web apps are as rich a target for bot attacks as they ever were.

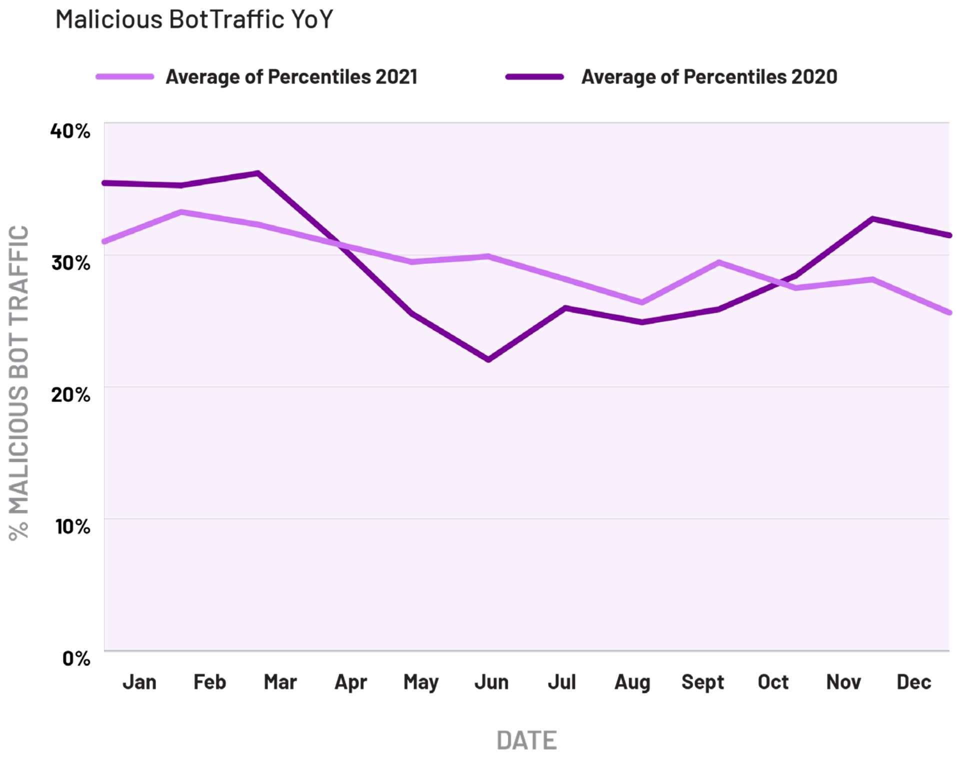


Figure 2: Percentage malicioius bot traffic out of total traffic in 2020 and 2021

Malicious Traffic Spikes

→ Drilling into the attacks that occurred each month offers even more insights into the pervasiveness of bad bots. Spikes of malicious traffic made up more than 50% of total traffic during monthly attack peaks for nine of the 12 months monitored, with peak bad traffic surpassing 95% in one month. This indicates that automated attacks regularly sent overwhelming amounts of traffic to some web applications, almost on par with a distributed denial of service attack.

But the amount of bot traffic doesn't correlate to its severity. In fact, sophisticated bots purposely keep attack volumes relatively moderate and dispersed over time to better blend in with legitimate traffic. This enables them to avoid triggering warnings and evade detection.

Attackers are increasingly diverse in their sophistication and attack methods. This includes technically adept youngsters, amateur botters, savvy professional cybercriminals and cybercrime communities, as well as a growing crime-as-a-service (CaaS) ecosystem that allows just about anyone to get in on the action. And they're turning their attention to e-commerce sites as the perfect vehicle to validate stolen information, make fraudulent purchases and steal the stored value in consumers' accounts.

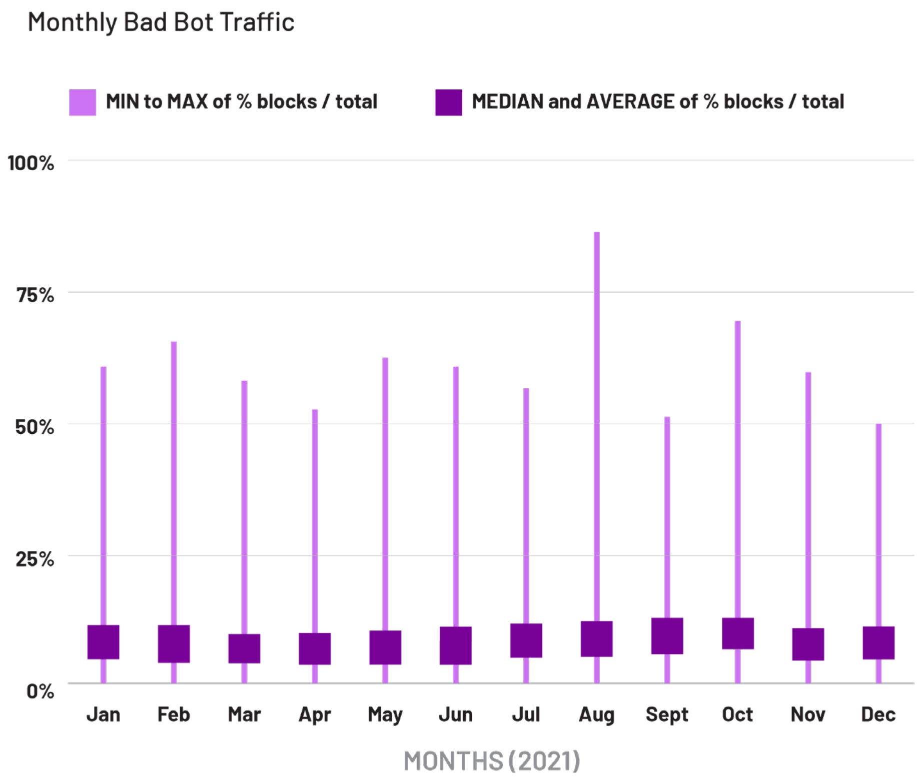


Figure 3: Percentage of bad bot traffic out of total traffic in each month, from minimum to maximum

Bot Traffic by E-commerce Segment

→ The retail e-commerce industry encompasses everything that is sold online, including apparel, electronics, furniture, toys and food, to name a few. Health and Wellness e-commerce companies were hit hardest by bot attacks in 2021, with 36.28% of total traffic coming from bad bots. This was followed by Hardware, Software and Electronics (33.2%) and Sports and Recreation (27.9%).

Bad bot traffic to Health and Wellness companies can be explained by increased activity in this space during the pandemic. As more people began using apps to purchase health-related goods, cybercriminals turned their attention to the Health and Wellness space — mostly to take over accounts and scrape pricing and product information.

The Hardware, Software and Electronics and Sports and Recreation segments include electronic devices and limited-edition sports apparel, respectively. This makes them a prime target for scalping bots, which primarily target specific products and brands. This leads to a bump in bot traffic to retailers that sell those coveted products.

Despite having lower bot traffic overall, companies in the Home, Kitchen and DIY and Fashion and Beauty segments experienced more credential stuffing and account takeover (ATO) attacks than other areas of e-commerce. This is likely because accounts with those companies are more likely to contain gift card balances, and gift cards to brands in those segments have a higher resale value.

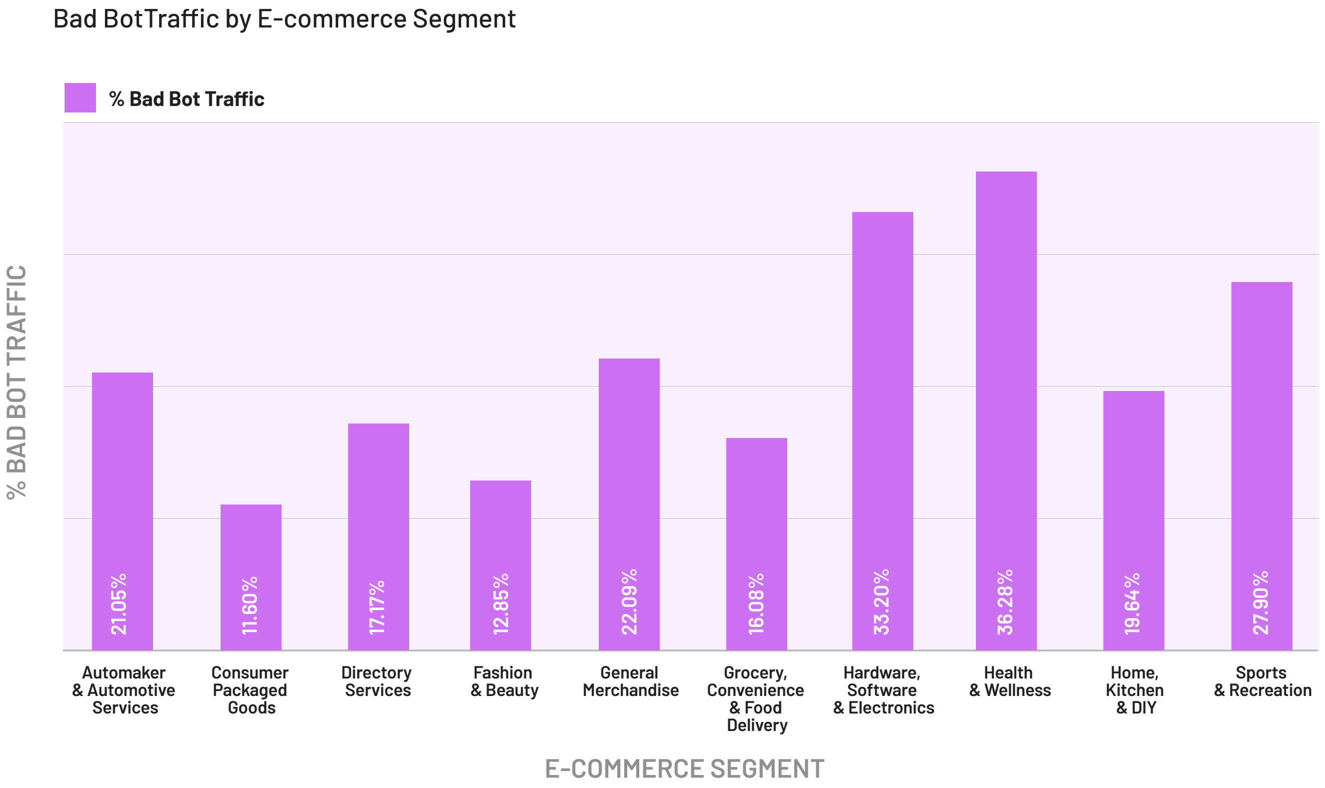


Figure 4: Average bad bot traffic out of total traffic as measured for the 75th percentile of each segment

Scraping

→ Scraping attacks were relatively stable throughout 2021. Scraping bot activity remained between 23% and 26% of total traffic for most of the year. It peaked at 27.77% of total traffic during the holiday season, when the competition among e-commerce sales events is at its fiercest. All in all, scraping bots comprised 25% of total traffic to e-commerce companies in 2021, which translates to an increase of 240% YoY in terms of total normalized requests.

Unlike other types of automated fraud such as carding or account takeover, scraping attacks rarely make the news — but that doesn't mean they don't harm your business. Here are a few ways that scraping bots cause problems:

- Skew your analytics and user behavior data, resulting in flawed decision making in key areas such as pricing, inventory, and marketing and advertising investment
- Tax you infrastructure and raises your cost for bandwidth
- Slow site performance, which frustrates customers
- Damage SEO rank if search engines detect duplicate content

Research indicates that the annual business impact of website scraping on e-commerce businesses is between 3.0% and 14.7% of annual website revenue, with a median of 8.1%.[2] This can negatively impact profit margins for online commerce providers by as much as 80%.

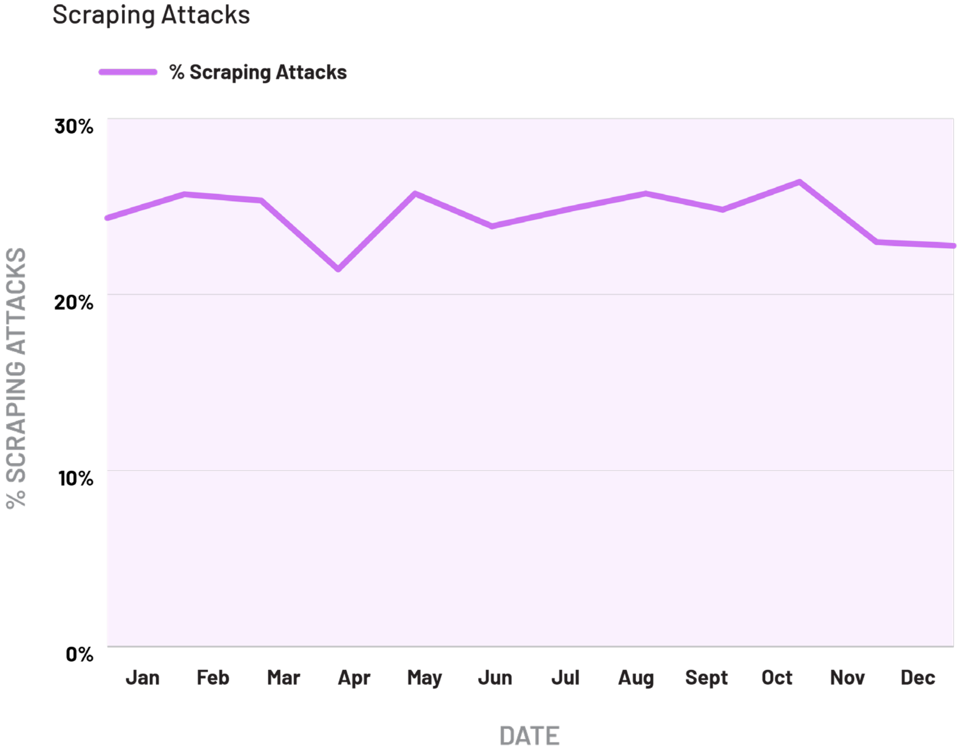


Figure 5: Scraping attacks against product and search pages as measured for the 75th percentile

Carding

→ The percentage of carding attacks out of total checkout attempts rose steadily throughout much of 2021, averaging 5.06% over the course of the year. This represents a 111.61% increase in terms of total normalized requests. Successful carding attacks cause financial losses because businesses must refund customers, replenish inventory that was delivered to cybercriminals and pay chargeback processing fees. As a type of checkout fraud, carding can also impact PCI compliance.

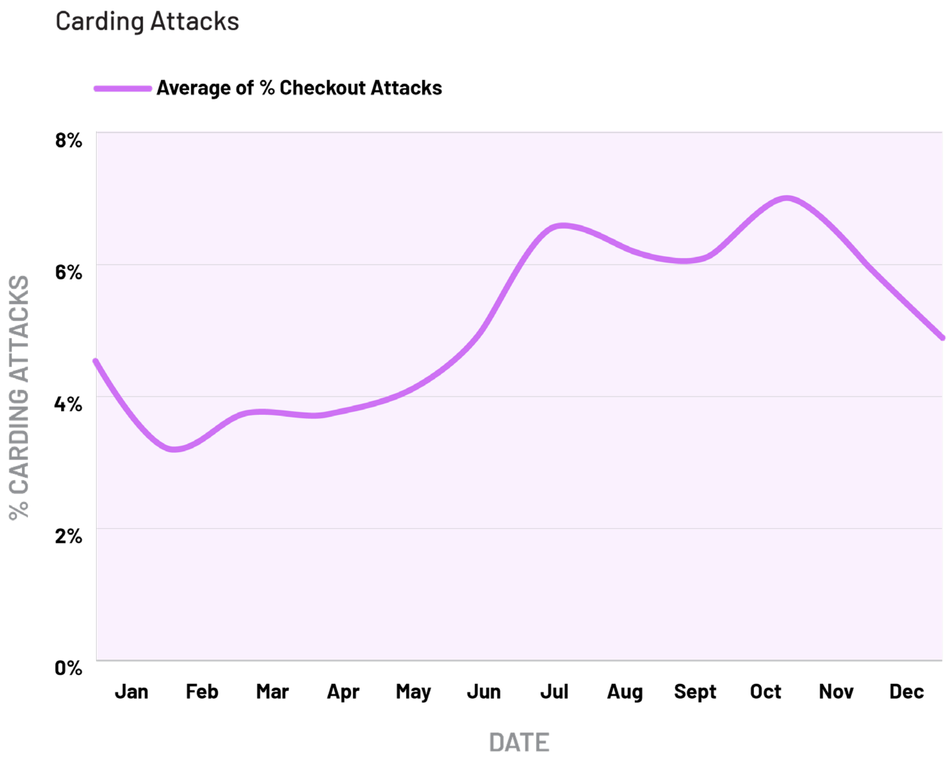


Figure 6: Average percentage of carding attacks out of total checkout attempts

→ Historically, many online retailers have considered carding fraud as just "a cost of doing business." That mentality is starting to change, with newer research showing the material impact of automated fraud. A recent report by Aberdeen Research found that an average 18-23% of e-commerce revenue is negatively impacted by bad bots each year. [3]

Credential Stuffing and Account Takeover

Malicious login attempts out of total logins trended upwards during 2021, reaching 93.8% of all login attempts in August. This is an 8% increase from the 2020 peak. Except for a small dip in the beginning of the year, attacks have remained above 75% of all login attempts.

Credential Stuffing and Account Takeover Attacks

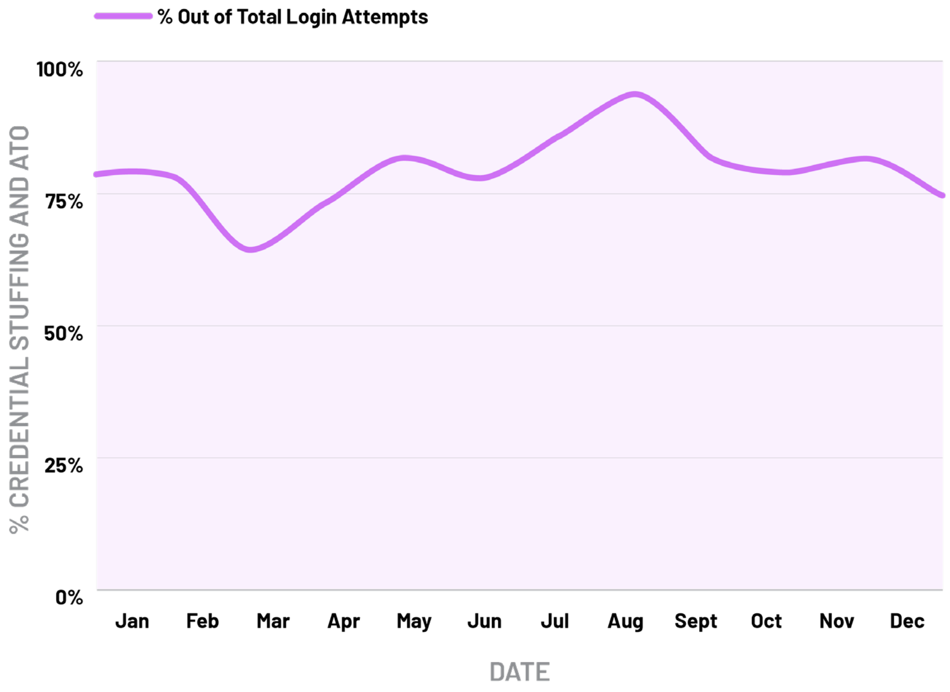


Figure 7: Percentage credential stuffing and account takeover attacks out of total login attempts measured for the 75th percentile

Credential stuffing and account takeover (ATO) attacks are a one-two punch — sometimes three or four punches. 65% of people reuse passwords[4] across multiple e-commerce sites, which means that stolen credentials can be used to access accounts on many different sites. And even if a password is changed on one site following a breach, it can likely still be used to access another. Even if a credential stuffing attempt is stopped, the cycle of damage will continue unless the entire web attack lifecycle is addressed.

Scalping

→ Scalping tends to be more targeted to specific brands than other types of attacks. Sure, anyone can buy anything to resell at a profit, but cybercriminals usually have bots go after hot products: limited-edition sneakers, gaming consoles, collectible cards and coins, concert tickets, popular toys and more recently, NFTs.

Looking specifically at online retailers that sold those high-demand products last year, scalping attacks were more than four times as prevalent as the industry average. Scalping bots comprised 40.13% of total checkout requests for hot products, while the percentage over all e-commerce segments was 8.32%.

Scalping attacks on high-demand products peaked at 71.61% of shopping cart requests on December 18, 2021 — a contrast from the 2020 peak of 46.87%. It was followed by several smaller peaks throughout the month. These spikes correspond to the sales that took place during the holiday shopping season.

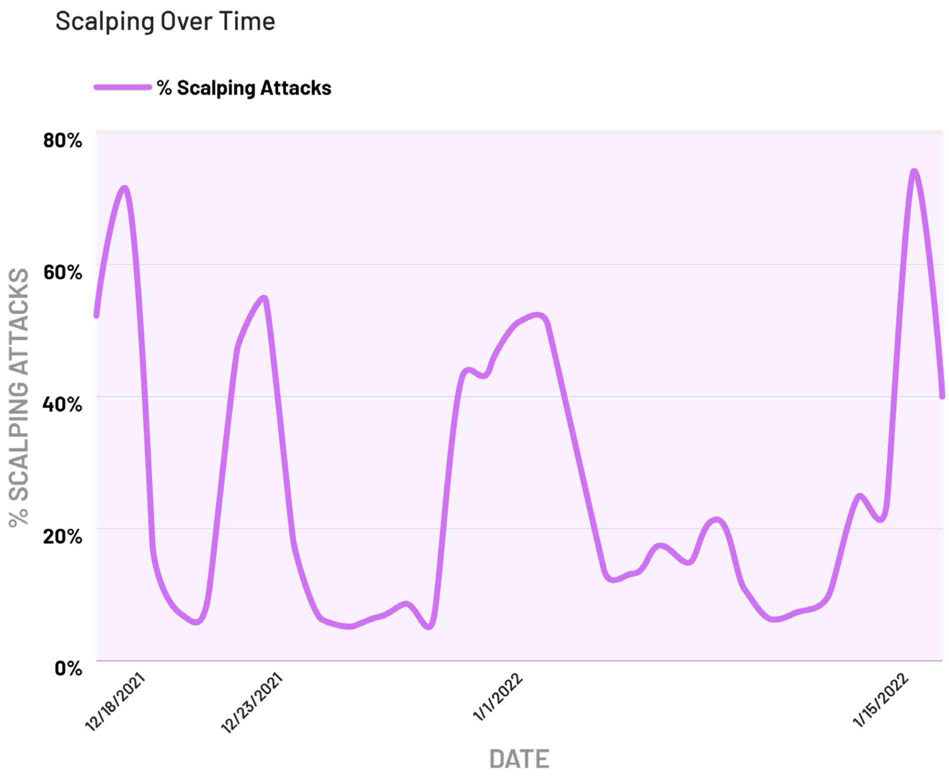


Figure 8: Percentage carding attacks out of total checkout attempts

Mobile vs. Desktop

→ Mobile traffic has been steadily increasing in recent years. In 2021, legitimate users were fairly split on how they accessed e-commerce sites: nearly 50% of traffic came from desktop devices and just over 50% came from mobile devices.

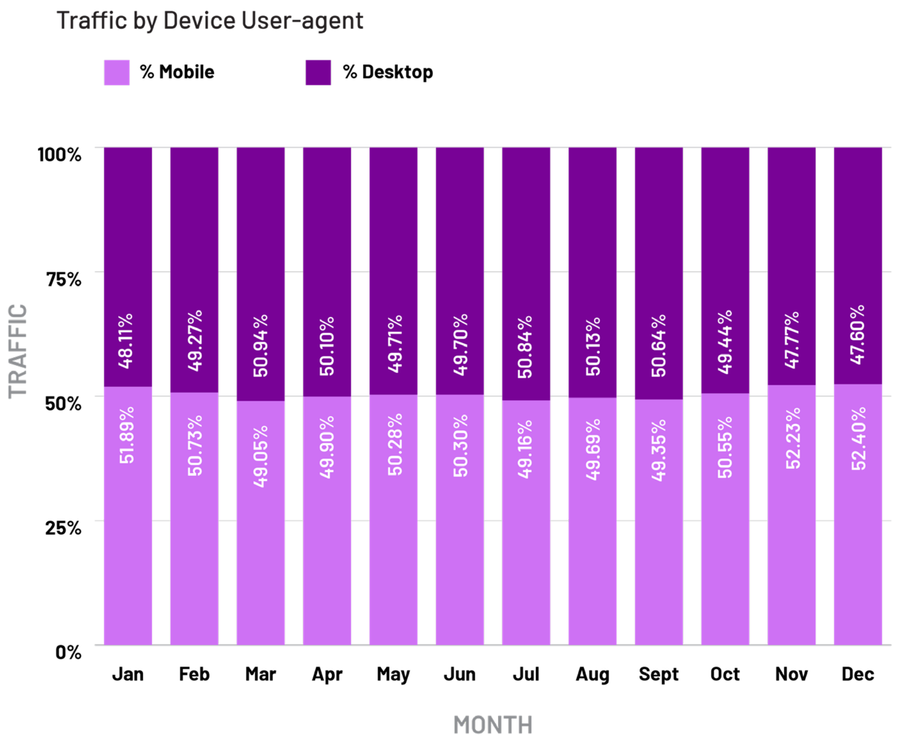


Figure 9: Distribution of traffic by device user-agent

→ Malicious bot traffic was another story. In 2021, roughly three-fourths (74.7%) of malicious requests came from desktop device user-agents and one-fourth (25.3%) from mobile user-agents. This means that attackers were disguising their attacks as desktop users almost three times as often as mobile users, but there is no certainty as to the actual devices being used in attacks because user-agent can be faked.

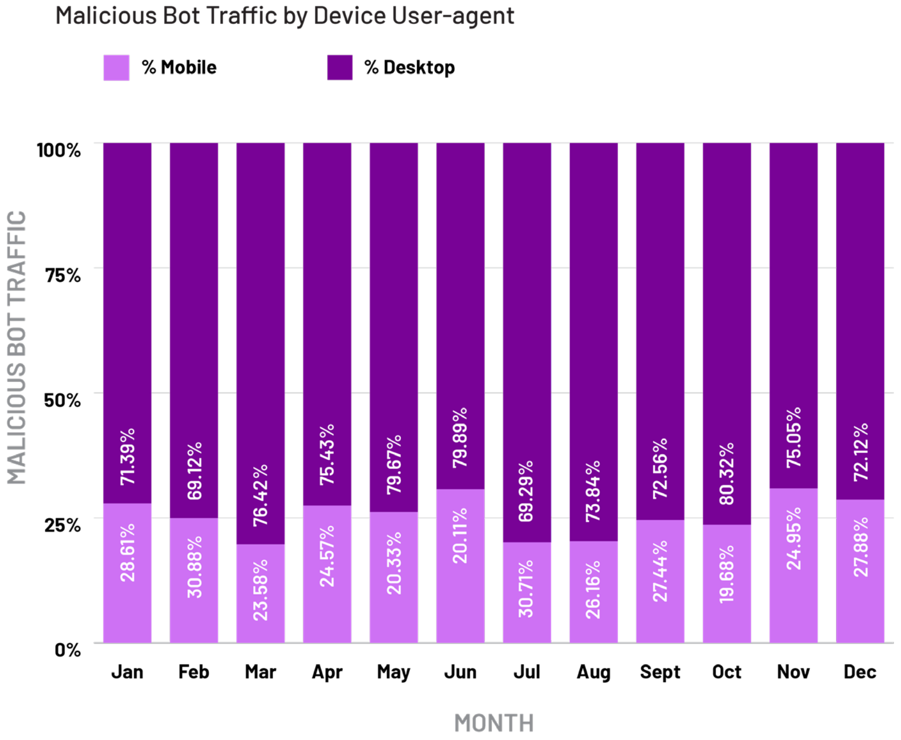


Figure 10: Distribution of malicious bot traffic by device user-agent

Bot Traffic by Country

→ Most malicious bot traffic originated from the U.S. and Canada, though these were also the top sources of traffic overall.

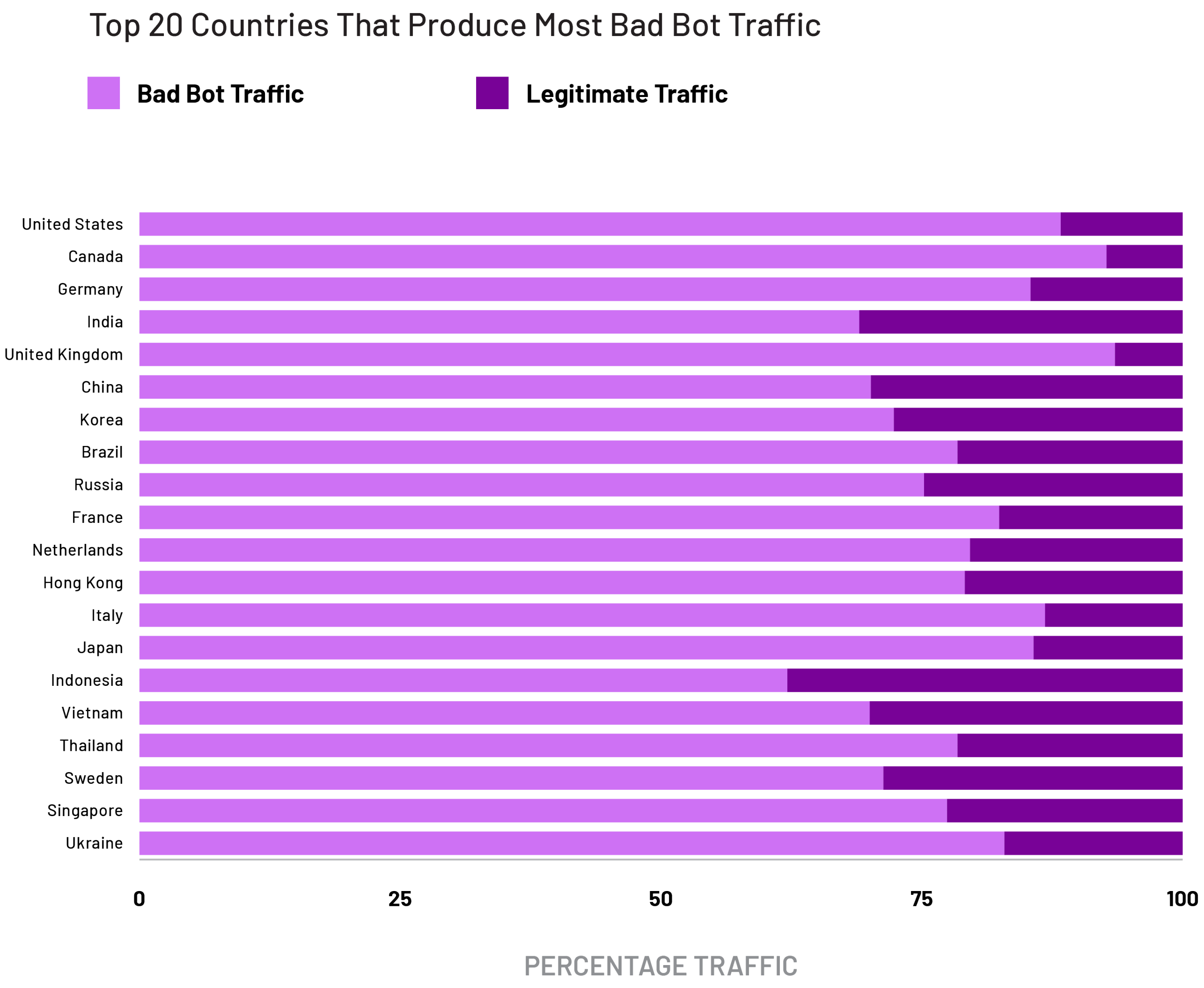


Figure 11: Distribution of traffic from top 20 countries by traffic type

→ Separating out each country reveals the geographies that produced the greatest amount of bad bot traffic out of total traffic coming from the region. The Åland Islands, an autonomous region of Finland, was number one with 71.88% bot traffic. This was followed by the Solomon Islands in Oceania (64.73%) and Burundi (64.68%). Although these places may look surprising, such locations generally have a lot of web proxies and hosting services that cybercriminals use to carry out attacks.

5.

Conclusion

→ A retailer's website is its digital headquarters. It is how consumers interact with the brand to browse inventory, read reviews, chat with customer support and ultimately, make a purchase. But it is also the doorway to a treasure trove of value — one that attackers are constantly trying to unlock with the help of automated bots.

When customers create a digital account, enter their credit card number and make a purchase online, they are placing their trust in the business. And that trust will be damaged if your brand fails to stop bot attacks and account abuse.

Here are a few steps you can take to prevent automated fraud:

- **Assess your risks:** Conduct an audit of malicious activity on your applications, including malicious login attempts, checkout attacks and overall bad bot traffic.
- **Identify target pages:** Make key product pages harder to scrape by using JavaScript elements or other techniques to slightly modify page code and composition.
- **Review your security infrastructure:** Identify the strengths and weaknesses of your existing tools. Web application firewalls (WAFs), for example, can stop the OWASP Top Ten, but not sophisticated bots that mimic human behavior or botnets that rotate through thousands of different IP addresses.
- **Analyze impact on consumers:** Some tools, such as CAPTCHAs or multifactor authentication (MFA) add friction to the user journey, causing frustration and driving cart abandonment.
- **Protect your revenue and reputation:** Leverage machine learning and behavioral analysis to detect and mitigate malicious bots without adding friction to the buyer journey.

6. Success Stories

"When it comes to detection, nobody does it better than HUMAN. They make sure the bots get all the friction without touching the customer experience."

-**Security Engineer**, Global E-commerce Retailer

Read case study →

"In just one hour of one day, if we had not had HUMAN in place, we would have seen about 34,000 hits on our backend payment processor. That's about $3,100 in fees."

-**Lee Tarver**, Senior Manager of Information Security Architecture and Engineering, Sally Beauty

Read case study →

"We frequently mention that HUMAN is part of our tech stack because we have seen first-hand how effective it is in keeping our customer data secure."

-**CTO**, Laybuy

Read case study →

Sources

[1] https://www.wired.com/story/dark-web-credentials-roger-stone-blueleaks/

[2] https://www.humansecurity.com/hubfs/HUMAN_Report_Aberdeen_The-Business-Impact-of-Website-Scraping.pdf

[3] https://www.humansecurity.com/hubfs/HUMAN_Report_Aberdeen-Impact-of-Bad-Bots-on-Ecommerce-Profitability.pdf

[4] https://services.google.com/fh/files/blogs/google_security_infographic.pdf

About Us

HUMAN is a cybersecurity company that safeguards 465+ customers from digital attacks, including bots, fraud and account abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.