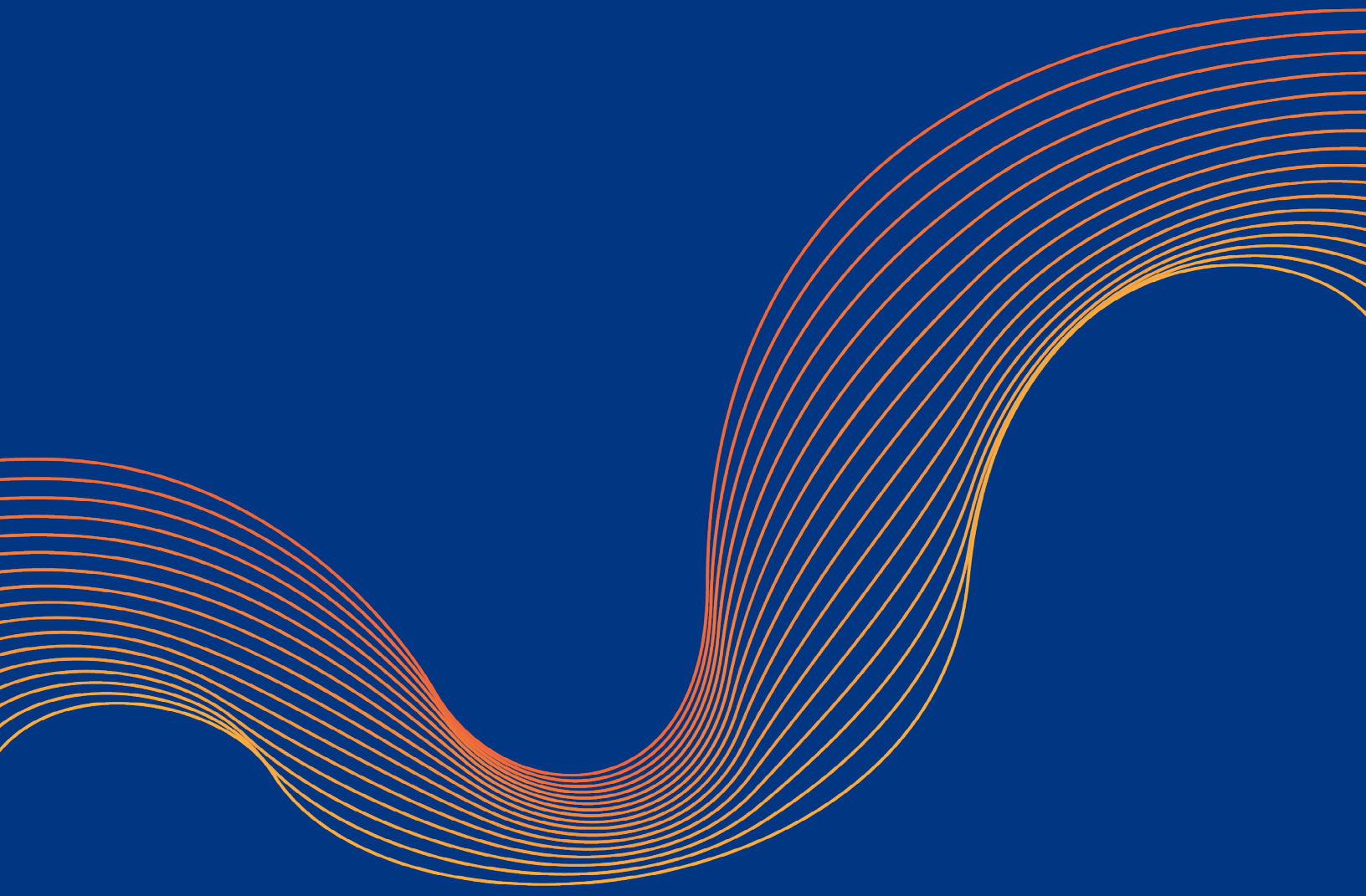
WHITEPAPER

CLOUDFLARE

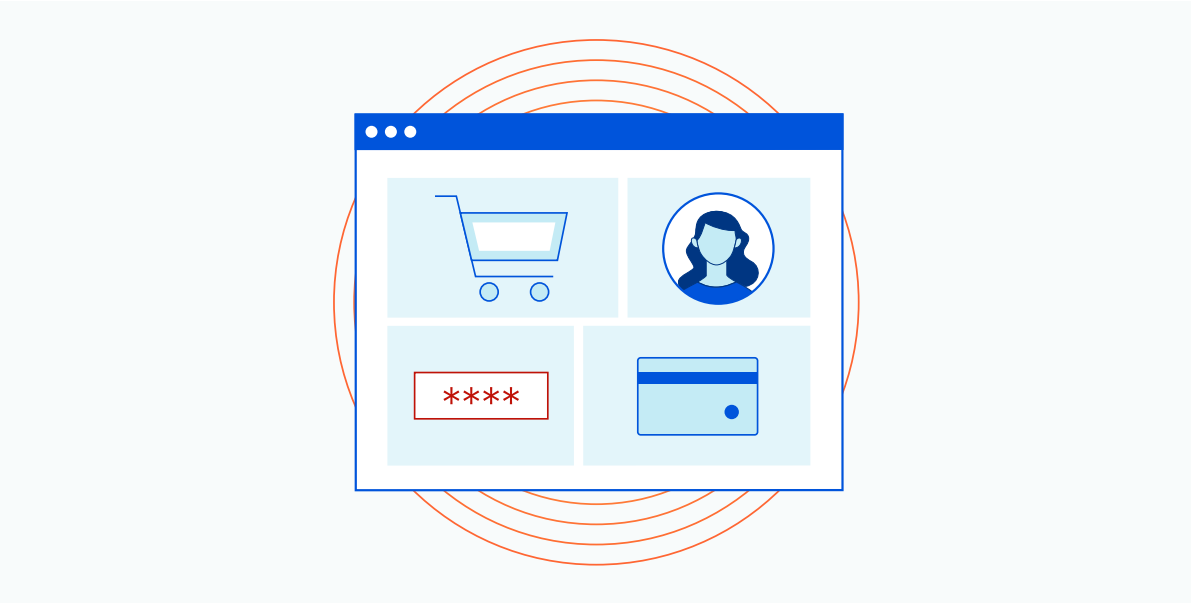
Malicious bots to look out for this holiday season



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

The 2020 holiday season seems primed for an increase in ecommerce spending. A recent Deloitte survey found that online shopping is projected to account for 64% of consumer spending in 2020, compared to 59% in 2019.

The survey also offers reasons to be optimistic about economic turmoil stemming from the Covid-19 pandemic. This turmoil is projected to slightly reduce holiday spending overall, but many of these expected losses stem from reduced travel expenditures — with clothing and home furnishing spending projected to increase by 12 percent year-over-year.



While these projections are good news for ecommerce companies, they come with a downside: the threat of increased malicious bot activity.

Malicious bots have of course plagued the holiday shopping season for some time. Ecommerce traffic can increase by as much 200% during peak holiday shopping weekends, Cloudflare data shows. Some bot attackers see these surges as an opportunity for automated traffic to go undetected.

And this year in particular, Covid-19 and remote work have put extra strain on IT and security teams. Cloudflare has observed increases in Layer 3 and 4 DDoS attacks since the beginning of the pandemic. Ecommerce companies should keep an eye out for similarly opportunistic increases in bot activity.

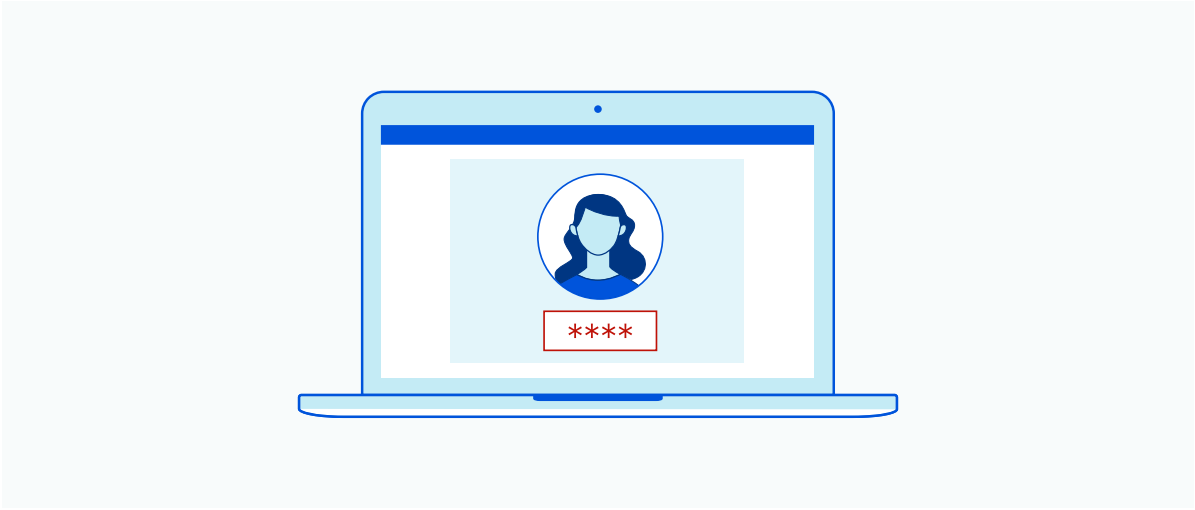
This paper describes three types of malicious bot to look out for this holiday season, and lists early warning signs that can help you detect such attacks:

- **Credential stuffers:** Which use stolen login credentials to access customer accounts.
- **Inventory hoarders:** Which fraudulently fill online shopping carts with in-demand products.
- **Price scrapers:** Which acquire product pricing information en masse for competitive purposes.

Credential stuffing bots

Credential stuffing is a type of brute-force attack. In this attack, a bot targets a login portal — such as the portal for an online shopping account — with many login credentials stolen from another site, in the hopes that a small fraction of them will work.

Credential stuffing relies on the tendency of website visitors to reuse usernames and passwords across multiple sites. For this reason, credential stuffing's success rate can vary drastically. However, the sheer volume of the credential collections being traded by attackers can make credential stuffing worth the effort. For example, in early 2020, the supermarket chain Tesco had to replace over 600,000 loyalty program accounts after a credential stuffing attack.



A credential stuffing attack typically follows the following steps:

1. An attacker acquires a large list of usernames and passwords that were stolen in a data breach.
2. The attacker designs one or more bots to test each of these username and password combinations on the targeted site's login portal, under the assumption that some of the combinations apply across multiple sites.
3. When a set of login credentials works, the attacker uses the account for malicious purposes. In an ecommerce context, this often means making fraudulent purchases, stealing credit card information, or stealing personal information that can be used in a phishing attack.

Ecommerce sites are popular targets for credential stuffing attacks because many online shopping accounts contain valuable financial information like credit card numbers and billing addresses. Credential stuffing attacks can be difficult to notice during the holiday season because of spikes in legitimate traffic.

Warning signs of credential stuffing attacks:

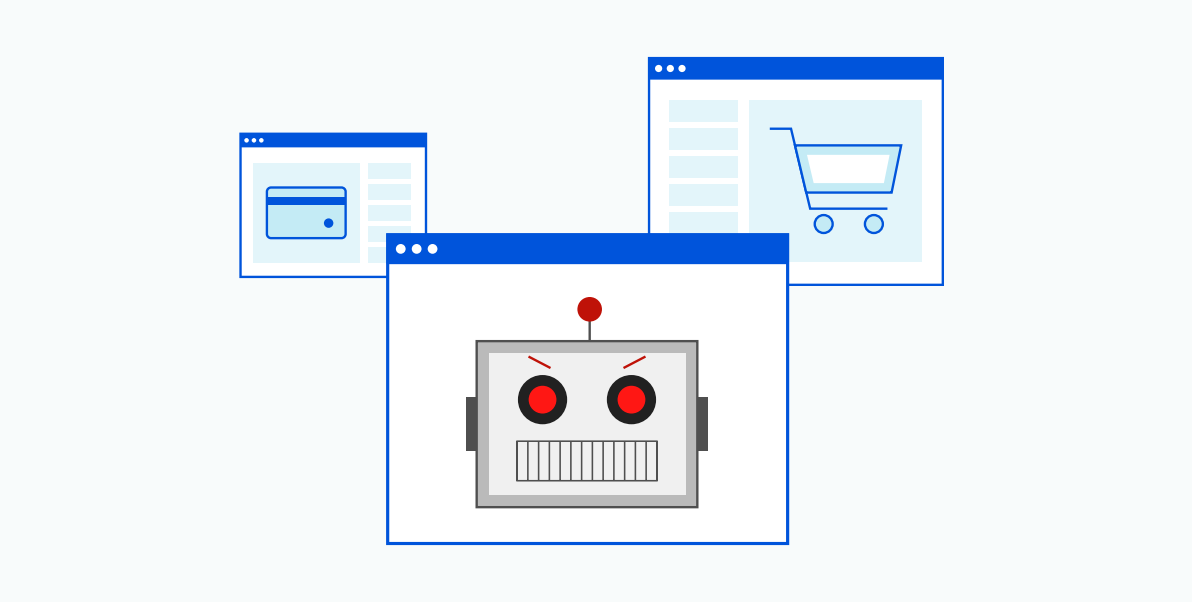
Ecommerce organizations should keep a close eye out for the following signs:

- **Increases in failed login attempts.** Be extra cautious about increases that come during times when customers don't typically shop, or come from unusual geographic locations.
- **Increases in changed credentials, addresses, and phone numbers.** If a credential stuffing attacker aims to make fraudulent purchases, they might edit this information in order to acquire their products — and to keep the real customer from finding out about the theft.

Inventory hoarding bots

Inventory hoarding bots disrupt the availability of ecommerce product inventory. They are commonly used for one of two purposes:

1. Purchasing in-demand products before human shoppers are able to, so the products can be resold on the secondary market for a higher price. 'Sneaker bots' are a well-known example of this tactic — they are often specifically designed for a particular website.
2. Adding high-demand products to an online shopping cart, but not buying them. To human shoppers, the product seems to be sold out — denying revenue to the ecommerce company, and making human shoppers more likely to buy the product from a competing site.



Inventory hoarding bots can be especially risky during the holiday shopping season. Entire products lines appearing to be sold out can scuttle crucial holiday sales, and waste the marketing investments supporting that sale.

Inventory hoarding also presents season-agnostic risks. Customers who are unable to acquire a product could develop negative feelings towards the merchant. And some inventory hoarding bots use stolen credit cards to make purchases, putting the merchant at risk of making no money on their supposed sale.

Warning signs of inventory hoarding bots:

This holiday season, ecommerce organizations should look for signs like:

- **Unusually fast purchases of low-volume, high-demand inventory.** This sign shouldn't come as a surprise — but as a basic best practice, ecommerce organizations should give these types of products extra scrutiny.
- **Customer complaints on social media.** Though checking social media requires manual effort, ecommerce organizations should keep an eye out for complaints about being unable to purchase especially desirable products.

Price scraping bots

Attackers use the price scraping bots to acquire product pricing information at scale and gain a competitive advantage.

Price scraping bots take a similar approach to other forms of content scraping:

1. The scraper bot sends an HTTP GET request to a targeted ecommerce website.
2. When the website responds, the scraper parses the HTML document for a specific pattern of pricing data.
3. Once the data is extracted, it is converted into whatever specific format the scraper bot's author designed.

With this data, competitor organizations can gain deep insight into an ecommerce site's pricing strategy.

Price scraping bots are especially dangerous during the holiday season for two reasons. First, pricing strategy is valuable information. If one organization knows all of its competitors' prices, they can consistently undercut the competitor—reducing the effectiveness of the competitor's holiday sales.

In addition, when price scraping bots visit large numbers of product pages, they skew pageview and conversion statistics. Web teams might draw mistaken conclusions about customer interest in certain products, or about the efficacy of special offers and other calls-to-action on those pages.

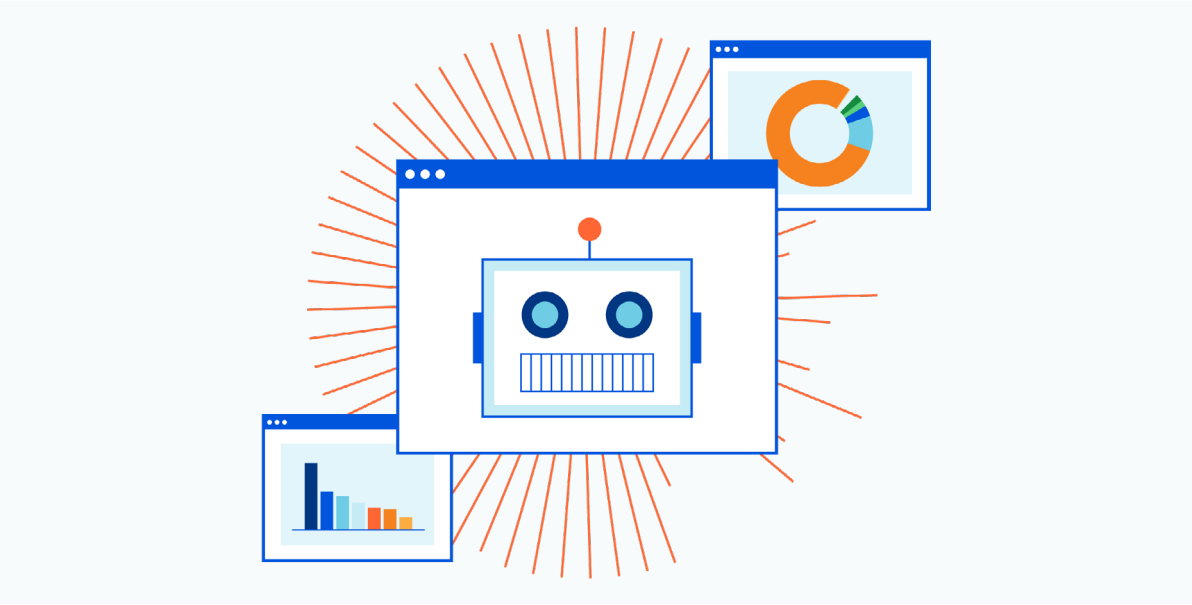
Warning signs of price scraping bots:

Price scraping bots can behave similarly to bots that crawl pages for helpful purposes like search engine indexing. To detect scrapers — and tell them apart from good bots — ecommerce organizations should keep an eye out for:

- **Slowdowns on a wide range of product pages.** Over-eager price scraping bots can strain an origin server's ability to respond to legitimate requests.
- **Page visits from unusual locations, at unusual times.** As with credential stuffing bots, these patterns can help you distinguish price scrapers from real shoppers.
- **Large numbers of advanced on-page actions.** Price scraping bots can take actions like filling out forms or clicking on buttons to reach certain parts of a website, whereas crawlers typically will not.

Bots are becoming more advanced

The previously mentioned warning signs are a good start for any bot management program. However, some bots are harder to detect. As you prepare your bot management approach for the holiday season, remember that bots can use tactics like:



- **Using web browsers to appear more like humans.** Google's Chrome browser is a popular choice, since it regularly accounts for over 50% of desktop and mobile traffic, based on data from the Cloudflare network.
- **Using multiple IP addresses to get around rate limits.** To block bots, many web forms limit the ability of any one IP address to make requests. But some bot operators use a botnet of compromised devices to avoid these limits.
- **Obscuring the originating network.** Some bots edit the packet headers of their requests to make it seem like requests are coming from a trustworthy source.
- **Changing tactics.** In addition to the tactics mentioned above, Cloudflare has also observed bots changing the times during which they act, slowing down request rates, and switching browsers—all to avoid detection.

For these reasons, isolated point solutions like rate limiting, CAPTCHAs, or WAF rules often offer incomplete protection against persistent bot attacks.

How Cloudflare can help with bot management

Cloudflare Bot Management helps organizations stop all of these types of bots in their tracks. The bot management solution is incorporated into the broader Cloudflare network, which supports approximately 25 million Internet properties and spans more than 200 global cities. By drawing on continuous threat intelligence from across that network, Cloudflare Bot Management offers behavior analysis, machine learning, and fingerprinting to remove much of the effort of combating bad bots.

For more information, visit **cloudflare.com/products/bot-management**.