The Quadrillion Report: 2024 Cyberthreat Benchmarks

HUMAN

The Quadrillion Report: 2024 Cyberthreat Benchmarks

Table of Contents

1 Introduction 3

2 Executive Summary 4

3 Attack Trends 6

4 Industry Trends 15

5 Cybersecurity Trends 21

6 Conclusions & Next Steps 26

7 Research Methodology 28

1.

Introduction

Every year, the Human Defense Platform observes more than *one quadrillion* (that's a one followed by fifteen zeroes) interactions across the internet. That's an immense amount of data to process, but simultaneously, it's a massive sample of activity on the internet from which to uncover how, where, and when threat actors are working to undermine attack surfaces along a customer's journey.

Users are at risk during every stage of the customer journey, from viewing and interacting with digital advertising to creating an account and logging in to completing a transaction. Today, more than 500+ customers and organizations trust HUMAN to protect them and their customers from those threats.

HUMAN's researchers examined the more than 1,000,000,000,000,000 interactions from calendar year 2023 to uncover new, emerging, and continuing threat patterns and tactics.

In this report, we'll explore trends in several common threat vectors, including:

- Account takeover attacks
- Fake account fraud
- Transaction abuse (carding attacks)
- Scraping

We'll also identify how certain industries are targeted by threat actors in specific ways:

- Web scraping attacks on retail and e-commerce websites
- Carding attacks on financial services websites
- Fake account creation on streaming and media websites

Finally, we explored some "big questions" about major industry topics, like artificial intelligence/language-learning models, loyalty and incentive program abuse, and the Internet of Things.

1,000,000,000,000,000

2.

Executive Summary

Let's share the baseline figures right off the bat:

In 2023, the Human Defense Platform blocked more than **352 billion attempts at account takeover**, carding attacks, and web scraping across HUMAN's customer base.

Researchers uncovered nearly **150 million new compromised credential pairs**, reflecting the continued value among hackers of account takeover attacks.

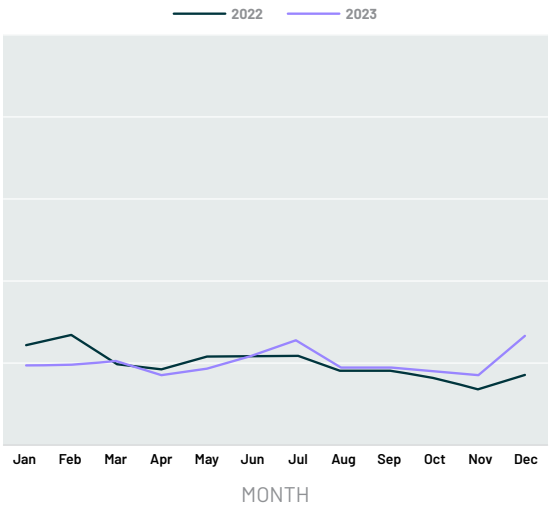
The rate of **account takeover attacks** in 2023 was about even with the rate of attacks in 2022, but the news was more dramatic for some industries. Financial services businesses saw the rate of ATO attacks **drop almost in half** (49% to 26% of traffic to login pages), but on the flip side, travel and hospitality businesses saw the rate of ATO attacks **jump from 32% of traffic on login pages to 52% of traffic**.

Account fraud attacks, including both fake account creation and account compromise after the point of login, are a new addition to this report. In 2023, HUMAN identified more than 200,000 fake account creation attempts per company and 40,000 compromised accounts post-login per company.

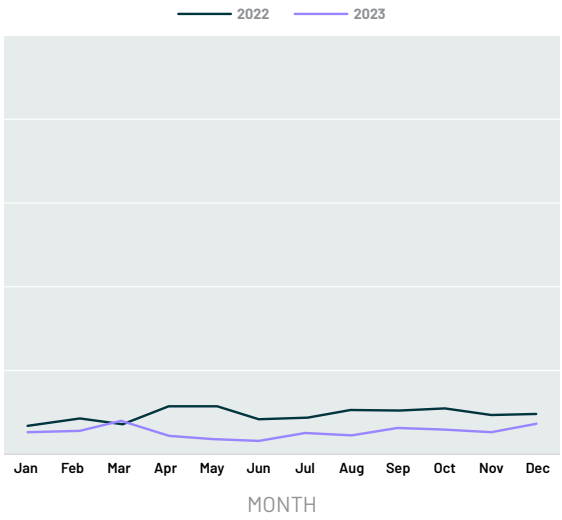
The rate of **scraping attacks** in 2023 remained high, with companies in the report experiencing more than one billion scraping attacks per company on average in 2023.

The rate of transaction abuse attacks, too, remained high from 2022 to 2023, to the tune of **46 million attacks per company in 2023**.

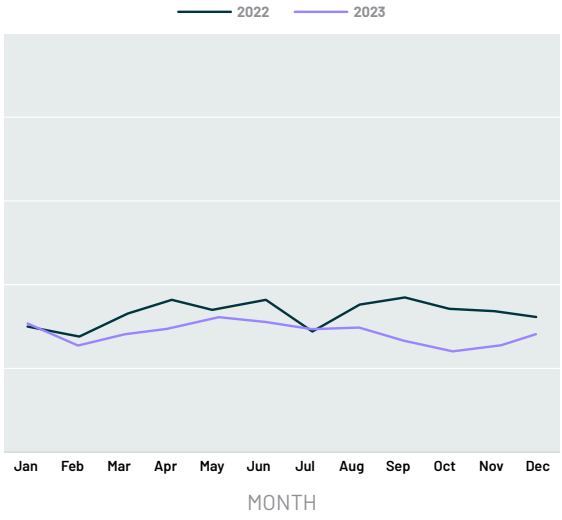
ATO Attacks in 2022 and 2023



Carding Attacks in 2022 and 2023



Scraping Attacks in 2022 and 2023



More insights on each of the above findings—as well as more industry- and threat-specific insights—appear in the following sections of this report.

The threatscape in 2023 continued to evolve as organizations put more defensive tools in place. Successful account takeover attacks, for example, require far more skills than they did only a few years ago. And since many individual hackers may not have all of the skills needed to carry out an attack at scale, the underground economy has consolidated into "firms" of diversified threat actors, each of whom has a part of the equation for an attack.

"This sort of attack group formation has been common for scalping attacks," said Aviad Kaiserman, a HUMAN Threat Intelligence Analyst. "This phenomenon has expanded from scalping to ATO, and bears monitoring."

Kaiserman also observed an increased focus among threat actors on reward programs. While these programs have always been lucrative for threat actors, the possibility of an economic downturn makes those loyalty initiatives even more compelling.

Finally, 2024 may feature more AI-based attacks than previous years. Satori Threat Intelligence analysts are monitoring AI-assisted credential cracking operations and processing of scraped content.

The following sections of this report explore all of the above in greater detail and offer key insights for businesses managing threats in 2024.

*The threatscape in 2023 continued to evolve as organizations put **more defensive tools in place.***

3.

Attack Trends

Enterprise-focused attacks observed by the Human Defense Platform fall broadly into one of several categories: account takeover attacks, account fraud, transaction abuse, client-side threats, and web scraping. Each of these buckets encompasses numerous attack paths, targets, and threat vectors, but all tend to incorporate some degree of automation.

The common wisdom is that bots make up a huge portion of internet traffic, possibly as much as half. With bots seemingly ubiquitous on the internet, is it any wonder they feature so heavily in cyberthreats?

In this section, we'll explore how we define these threats, how the Human Defense Platform observes and stops them, and how prevalent these attacks were in 2023. We'll also look at stories of attacks stopped to give a glimpse inside what it means to stop fraud.

Account Takeover Attacks

Account Fraud Attacks

Transaction Abuse

Scraping

Account Takeover Attacks

In an account takeover attack, a threat actor gains unauthorized access to a user's account. With this access, the threat actor then has a choice: take advantage of the access to account funds and balances or resell that access on an underground marketplace.

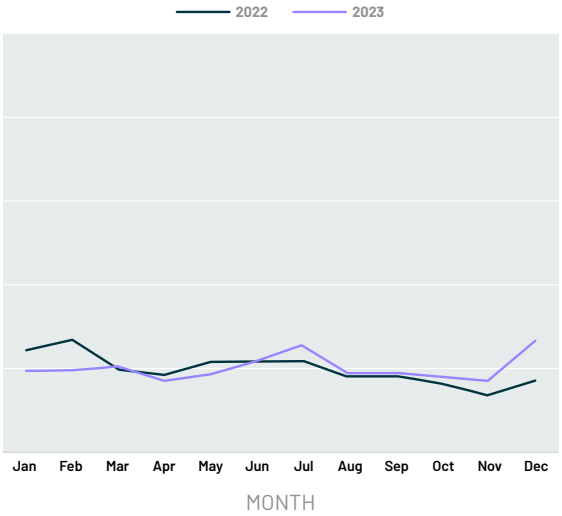
The final threat actor in the chain can then withdraw or transfer funds, make fraudulent purchases, steal payment data, collect personally identifiable information (PII), drain loyalty point balances, write fake reviews, or even distribute spam and malware.

Account takeover attacks most frequently happen as a result of a data breach: the harvested credentials are sold from one threat actor to another, and those credentials are peppered at login portals to find accounts whose users reuse passwords from one account to the next. **Credential stuffing attacks** (threat actors using leaked credential pairs on many login portals to find accounts that work) and **credential cracking attacks** (threat actors using partial credentials to try and brute-force a successful credential pair on a particular website) are the most common variants.

*HUMAN blocked more than **26 billion fraudulent login requests** over 2023.*

In 2023, account takeover attacks were **mostly level** to the previous year:

ATO Attacks in 2022 and 2023



While in 2022, attackers started hot, with nearly 25% of traffic to login pages in January and February being fraudulent, in 2023 that number (for those months, anyway) fell to about 20%. That said, even a 20% ATO ratio is nothing to laugh at: **one in five visits to a login page is a break in attempt**.

Attacks in 2023 crept up over the summer; indeed, more than half of the ten worst days for account takeover attacks in the entire year took place within June and July. Rates ticked down again to 2022 levels for the fall, but a significant spike took place at the end of the year. On the whole, HUMAN blocked more than **26 billion** fraudulent login requests over 2023.

HUMAN's Satori Threat Intelligence team reported that account takeover attacks evolve constantly in response to new security measures intended to stymie them.

"The more robust the security, the more complex the account takeover attack infrastructure has to be," said Aviad Kaiserman, Threat Intelligence Analyst. "With TLS checks, one-time passwords, rate-limiters, numerous varieties of CAPTCHA, two-factor authentication and verification codes all in play, attackers must undergo a much more extensive preparation phase and invest far more resources when planning an attack."

As account takeover attacks grow in complexity, attackers need to raise their skill level to include all of the tactics, techniques, and procedures (TTPs) needed to break through an increasing number of layers of security.

"This has led to an 'invisible hand'-like mechanism and the growth of underground economies dedicated to account takeover infrastructures," said Kaiserman. "In such an economy, there's a division of labor among specialists, each offering skills and resources to carry out an attack. For example, some solve CAPTCHAs, others create proxy pools, others figure out one-time passwords, and so on."

> **"As account takeover becomes a team sport, so to speak, potential targets will need to step up their game to identify how, when, and where those threat actors are likely to attack."**
>
> -**Gavin Reid**, CISO at HUMAN

Satori Story: Capra

In August 2023, HUMAN published a report[1] into a coordinated account takeover attack dubbed **Capra**. This attack targeted sports betting sites' login APIs, spoofing the OS from which the login attempt originated, solving a CAPTCHA, and breaking through a rate-limiting security protocol. Once an account was tested this way, access to account information was sold to other threat actors, along with tips for circumventing two-factor authentication.

The attack was brief: within a couple hours, the targeted platform observed the issue, found the source, and plugged the gaps in security. But the damage was done, as thousands of user accounts were drained in the meantime.

HUMAN's customer was protected from the Capra attack, while other platforms targeted by the attack were less fortunate.

Key Findings:

- **ATO attacks continued in 2023 at roughly the same rate as 2022, making up a little more than 20% of all login requests.**
- **HUMAN blocked more than 26 billion fraudulent login requests in 2023.**
- **In September 2023, one retailer experienced an account takeover attack during which fraudulent login attempts made up 99.58% of all traffic to the account login page.**

[1] Anatomy of an Account Takeover Attack: Capra. HUMAN.

Account Fraud Attacks

"Account fraud" is a broad category, including **fake account creation** (which itself is but one means to many ends) and **compromised accounts that occur post-login**.

An example of post-login account fraud: if your cookie for a particular retailer (a tiny file on your computer that tells the retailer's website who you are, letting them follow your account activity from one session to the next) is stolen, a threat actor could take over your account with that cookie. From there, the threat actor could wreak the same havoc as in an account takeover attack.

Account fraud attacks in 2023 break down into those two subcategories: fake accounts and post-login account fraud.

Satori Story: ScrubCrypt

In November 2023, HUMAN's Satori Threat Intelligence Team published new research into a tool called **ScrubCrypt**, which helps threat actors carry out account fraud attacks by obfuscating the malware they use to steal cookies and credentials.

ScrubCrypt, which was available for rental on dark web hacker forums, was used in conjunction with RedLine Stealer during an attack on one HUMAN customer. RedLine Stealer is a well-known malware that, when snuck onto an unsuspecting victim's device, retrieves cookies and saved credential information, reporting it back to the threat actor. ScrubCrypt, in this attack, was intended to help get RedLine Stealer past a user's antivirus protections.

HUMAN's customer was protected from this attack.

Average Volume Observed Per Company by Human Defense Platform

Fake Account Creation

218,460

Compromised Accounts

39,691

Kaiserman, a HUMAN Threat Intelligence Analyst, spoke about the role of fake account creation in incentive program abuse.

"If a site offers $5 for any member who refers a new member, an attacker can create numerous 'friends' accounts and generate a significant income from this reward program," Kaiserman said. "Alternatively, attackers can create a new 'identity' for themselves to take advantage of limited-duration free trials of a service, like on a streaming site, creating perpetual free access to the service."

More info on incentive and loyalty program abuses is in the later section on Cybersecurity Trends.

Key Findings:

- **HUMAN identified and flagged more than 218 thousand fake accounts per company created during 2023.**
- **Compromised accounts — in which real accounts are broken into as a result of an account takeover on another platform — accounted for 40 thousand account fraud attacks per company in 2023.**
- **Incentive programs that offer direct financial rewards are often a key cause of account fraud attacks.**

> **"... attackers can create a new 'identity' for themselves to take advantage of limited-duration free trials of a service, like on a streaming site, creating perpetual free access to the service."**
>
> -**Aviad Kaiserman**, Threat Intelligence Analyst at HUMAN

Transaction Abuse

If you've heard of (or worse, experienced) "**carding**," you've heard of transaction abuse. This threat model centers on testing stolen payment card information by making small purchases on e-commerce sites. Validated cards are then used for bigger purchases—often of gift cards/codes delivered electronically and immediately—which are in turn sold on hacker marketplaces, completing the fraud often before the user can do anything about it.

Carding is distinct from account takeover, account fraud, and web scraping attacks in one key way: attackers care a lot less about who they're targeting with a carding attack. Consider: the goal of the attack is to validate the card, after which they're off to the races. That validation can come from any target, and if getting it on Company A is too hard (because their security posture prevents such an attack from working), they'll go down the digital street to Company B.

In this way, potential targets for carding attacks can more easily get to a point at which they stop being an appealing target than they can for other attack types. Or, to use an analogy from the animal kingdom, they don't have to outrun the lion, they only need to be faster than the slowest wildebeest. And the penalties for being the slowest wildebeest include chargebacks, increased costs for payment processors, and direct penalties.

Client-Side Attacks: Magecart and Skimming

Carding is just one form of transaction abuse, and is in fact often the result of *another* form of abuse, one that occurs on the client's side: **skimming**.

You may have heard of **Magecart** — for a while, it was one of the biggest names in cyber attacks. But Magecart is the name of a loose collection of hackers, not of the type of attack itself. "Magecart attacks" are generally **digital skimming** attacks by another name.

Skimming occurs when a code is implanted on a business' checkout page (usually through a third-party's web extension or script), grabbing the payment card information and relaying it back to a threat actor. Skimming can be particularly hard to detect, as the attack doesn't hit the target business' tech stack, it's riding alongside a script running in the browser.

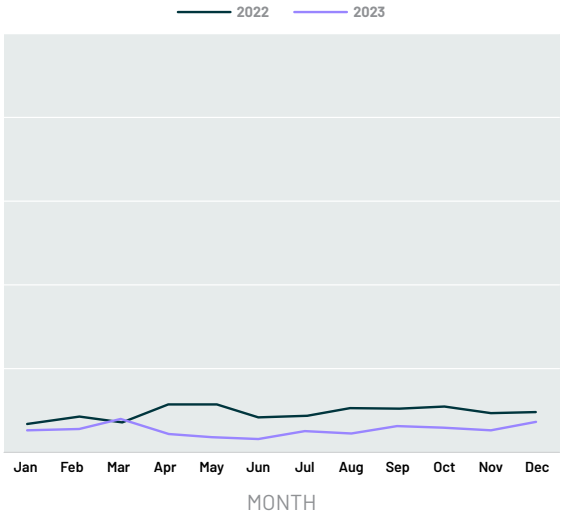
In a Magecart-style attack, threat actors mess with payment pages to change how the form fields work. There are a few ways of doing this, but the end result is the same: the cybercriminals steal payment card information and PII.

"Carding is especially pernicious as it's like dipping a toe in the water for a threat actor. If the water's fine, they're able to jump right in with that same stolen payment info on another site, making a much bigger splash."

-**Lindsay Kaye**, VP of Threat Intelligence at HUMAN

There's an interesting dichotomy in the figures around carding in 2023:

Carding Attacks in 2022 and 2023



The *rate* of carding attacks is down fairly significantly. In fact, only in one month (March 2023) was the overall percentage of attacks higher than the previous year (and even that only barely).

But the actual *total number* of attacks rose by **33%**, and the average number of attempted carding attacks per customer rose by **26%**. This suggests there's still enormous value to threat actors in carding attacks (it's free money, after all), but that these attacks aren't working very well.

Kaiserman, a HUMAN Threat Intelligence analyst, explains.

"2023 saw a significant increase in banking security precautions alongside digitization efforts," Kaiserman said. "When an attack becomes that much harder to carry out, attackers need to put more resources into it, which in turn makes it less profitable on the other end."

Key Findings:

- **The *rate* of carding attacks has dropped, but the *number* of carding attacks has risen. Satori researchers believe this is the result of new regulations for banking following digitization efforts.**
- **An enhanced security posture — including proof-of-work challenges or GPU challenges — can make a site a less desirable target for attackers.**

*In one attack on a retailer in May 2023, HUMAN found that **98.25% of checkout attempts were fraudulent**. HUMAN's customer was protected from this attack.*

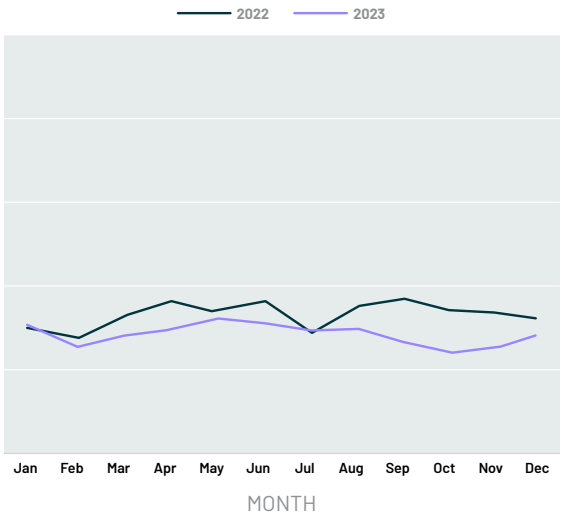
Scraping

Scraping — the phenomenon of bots arriving on a website, capturing a whole bunch of information, and leaving again — sounds like it shouldn't be too big of a problem: if the information is available on the website, how is a bot visiting any different from a human visiting? The answer is in what the bot is intending to do with that information:

- Competitors can use bot-gathered intelligence to undercut your business' strategy and pricing.
- Bots can hunt for staged-but-unreleased product listings to learn what's coming soon.
- Threat actors can repost scraped content to damage search engine optimization.
- Bots can identify and resell restricted content.
- Scraping can even lead to misinformed business decisions based on misleading website metrics and look-to-book ratios.

In 2023, web scraping attacks were roughly even with the previous year:

Scraping Attacks in 2022 and 2023



URL Paths and Web Scraping Patterns

HUMAN researchers looked at the URLs on which scraping attempts were most common, and some interesting patterns emerged:

- The most common non-homepage URL path scrapers targeted was /api. Scrapers may have been looking for ways to gather information — particularly from retail businesses — without visiting the public website.
- /ip was another very common URL path for scrapers. Some retailers include /ip in the URL path of product pages, and scrapers may have been hunting for product descriptions or pricing.
- /article, /flights, /transport, and /shop were also very common URL paths, all of which point to web scraping for content and pricing information.

Scraping Attempts

On average, HUMAN customers saw **more than one billion scraping attacks blocked** during the calendar year.

Interestingly, four of the five biggest days in 2023 for web scraping attacks were four consecutive days in October: the fifth through the eighth. During that time, **more than one in every three visits was a scraping attack**.

It's hard to draw concrete conclusions, since every website is built differently according to the needs of the technologies that support it, but a few things jumped out to Kaiserman, a HUMAN Threat Intelligence Analyst.

"Scraping on product and search paths could be any one of a few things: it might simply be content aggregators, price comparison tools, or business intelligence bots," Kaiserman said. "But they might also be hunting for new product listings or changes in stock levels to get ahead of humans who wouldn't have the same advantages."

*One HUMAN customer experienced an attack during which **98.55% of traffic to their website was attempting web scraping.** HUMAN's customer was protected from this attack.*

Key Findings:

- **While scraping as a percentage of traffic is down slightly from 2022, the number of attacks still averages over a billion scraping attack attempts per year per customer.**
- **Reducing scraping attacks can have downstream benefits, like protecting the integrity of marketing metrics or improving look-to-book ratios.**

4.

Industry Trends

The Human Defense Platform protects organizations of all kinds, from international retailers with thousands of brick-and-mortar locations to online sports betting platforms, from airlines to educational tutoring companies, and from SaaS providers to media outlets.

No two businesses have the same threats and the same risks. A financial services organization might be worried about account takeover attacks, while a retailer might be concerned about scalping or price scraping.

Even businesses that share an industry might have disparate concerns. Financial services organizations, for example, might find themselves at risk for both carding attacks and account takeover attacks, but not to the same degree as the institution down the street.

HUMAN researchers examined the patterns in attacks from an industry perspective to understand whether threat actors were changing their tactics. Here's what we found.

Travel & Hospitality

Retail & E-commerce

Financial Services

Streaming & Media

Technology, SaaS & Services

Travel & Hospitality

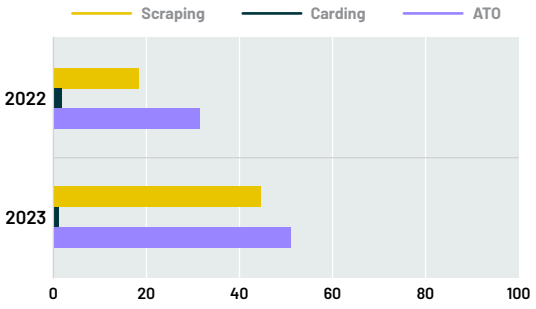
Businesses in this category are often targeted with several types of threats:

- Web scraping attacks (collecting pricing information and inventory changes)
- Account takeover attacks (for stored payment information, PII, and loyalty program balances)
- Account fraud attacks (to exploit new account bonuses)

While carding attacks stayed largely consistent from 2022 to 2023, account takeover attacks rose **20%**. The world continues to reemerge from the pandemic, and travel rose accordingly.[2]

Travel and hospitality tends to have a love/hate relationship with scraping. After all, travel website aggregators can't provide up-to-date information for flights and hotel reservations if they can't check those rates. But at the same time, those scrapers might exploit certain dynamic pricing or discount structures that aren't intended for broad consumption.

Travel & Hospitality Attack Rates – 2022 vs. 2023



PERCENTAGE OF WEB TRAFFIC ATTEMPTING ATTACKS

How Good Scrapers Self-Identify

Any time you visit a website, the website learns a few basic things about your tech setup: what browser you're using (and what version of that browser) and what operating system you're on (which can tell the website if you're on a laptop or a phone). But good web crawlers add a little bit more — they self-identify:

```
Mozilla/5.0 AppleWebKit/537.36 (KHTML, like
Gecko; compatible; Googlebot/2.1; +http://
www.google.com/bot.html) Chrome/120.0.0.0
Safari/537.36
```

Notice "Googlebot" in the string. This tells a website "don't block me, I'm just getting information so I can help people find you." And that's what a good scraper does.

Now, attackers know this too. They know what good web scrapers do, and they know how to make their bad web scrapers pretend to be good web scrapers. There's nothing to stop an attacker from trying to spoof real web crawlers, so businesses that benefit from good bots rely on the Human Defense Platform, which can distinguish the real web crawlers from the spoofed ones, blocking only the fakes.

[2] Number of international tourist arrivals worldwide from 1950 to 2023, Statista.

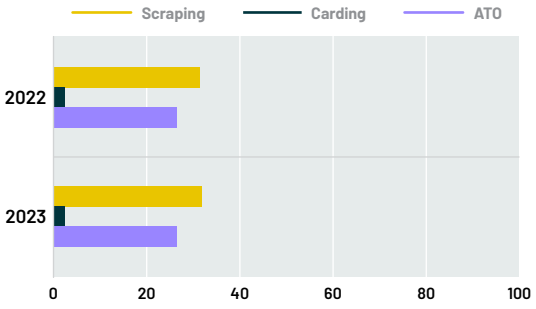
Retail & E-commerce

Retail and e-commerce businesses are among the most targeted businesses:

- Web scraping attacks (collecting pricing or product information)
- Account takeover attacks (for stored payment information and PII)
- Account fraud attacks (to exploit new account bonuses or loyalty programs)
- Transaction abuse (attempting small purchases to test and validate stolen credit card numbers to either resell or use to make large fraudulent purchases/buy fit cards)
- Magecart/skimming (to steal payment information)
- Collusion fraud (the misuse of a marketplace to launder money)

Account takeover attacks on retail and e-commerce businesses remained consistent (about **27%** of traffic on login pages) between 2022 and 2023. On the flip side, scraping attacks were — and remain — the biggest attack type targeting retail and e-commerce organizations.

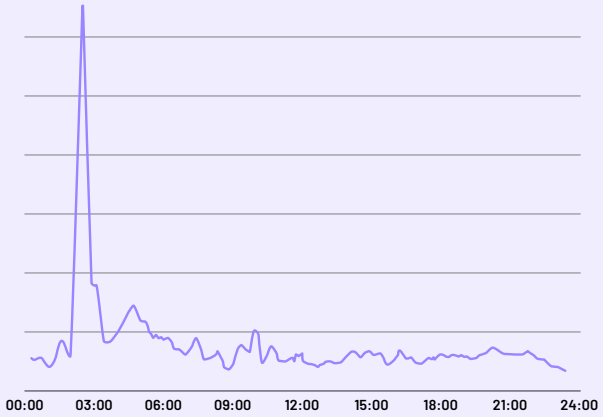
Retail & E-commerce Attack Rates – 2022 vs. 2023



PERCENTAGE OF WEB TRAFFIC ATTEMPTING ATTACKS

Malicious Traffic During a Product Drop

The public drop of a high-profile or in-demand item is its own beast, though. In one brief moment, the population of malicious bots on the website can spike dramatically:



TIME OF DAY – MARCH 28

This chart spans one day for one customer. When the sale began, the number of bots targeting the website jumped **more than 700%**. An hour later, the bots retreated, and the level of bot activity for the rest of the day returned to a normal level.

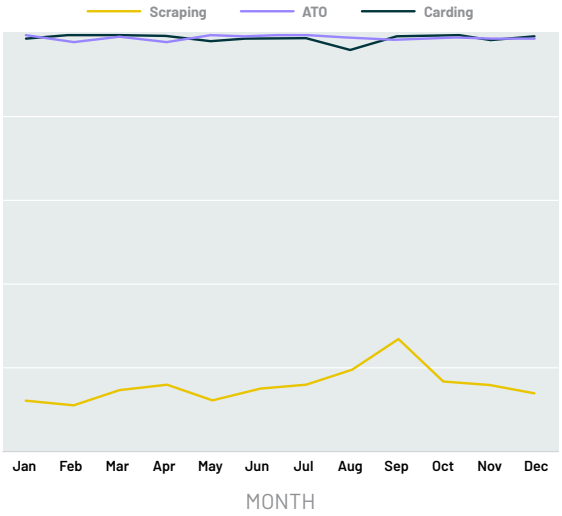
Financial Services

Due in no small part to the fact that there's money "available", financial services organizations experience a variety of attacks, largely focused on seizing that money:

- Account takeover attacks (to drain account balances)
- Account fraud attacks (also to drain account balances)
- Carding attacks (to test credit cards)
- Client-side attacks (to collect PII)

Unsurprisingly, account takeover and carding attacks were high-volume attack types for businesses primarily focused on managing users' money. A simply massive proportion of the traffic to the login and payment portals on these websites was attempting an attack:

Attack Types Against Financial Services



You're reading that right: nearly **99%** of the traffic to login and payment pages—even normalized for outliers, as described in the Methodology section of this report—was attempting to break into user accounts or steal information from a payment page.

Streaming & Media

Businesses in the streaming and media industry face a wide variety of threats:

- Carding attacks (to test cards with immediate feedback of success)
- Fake account attacks (chaining fake accounts to exploit new user discounts)
- Advertising fraud (depriving publishers of earned advertising revenue)
- Account takeover attacks (to steal payment card information)

With apologies to Mark Twain, reports of the death of the "streaming wars" have been greatly exaggerated.[3] While some outlets report that the battle for streaming supremacy has concluded, other platforms continue to offer free trials for new users, providing a juicy incentive for threat actors to chain one fake account after another in an effort to get the content but never pay the bill.

Account fraud and carding tend to be among media publishers' top concerns. The feedback loop for a successful carding attack is immediate (access to the content library is instantaneous) and many users might not even notice a fraudulent expenditure (as they may themselves be a subscriber to the same publisher/streaming service), slowing the time-to-detection and giving the threat actor a longer window within which to use the validated card.

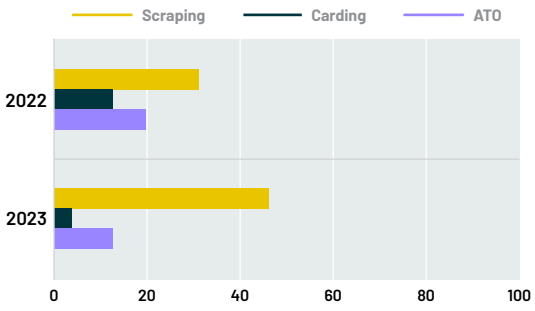
Streaming Fraud

In addition to the threats described, streaming services also contend with fraud tailored to their particular business model. Music streaming services face the possibility of **streaming fraud** (also known as spin fraud), in which an artist, album, or song is "listened to" by bot armies with the goal of driving that artist, album, or song up the charts.

Other emerging and growing formats like connected TV and in-game advertising face their own unique challenges as security and transparency initiatives race to catch up to and protect the new opportunities available to advertisers and agencies.

While account takeover attacks fell (**from 20% to 12%** of traffic on login pages) from 2022 to 2023, scraping attacks rose significantly (**from 31% to 46%**) and carding attacks fell (**from 13% to 4%**).

Streaming & Media Attack Rates – 2022 vs. 2023



PERCENTAGE OF WEB TRAFFIC ATTEMPTING ATTACKS

[3] Death hoax. Wikipedia.

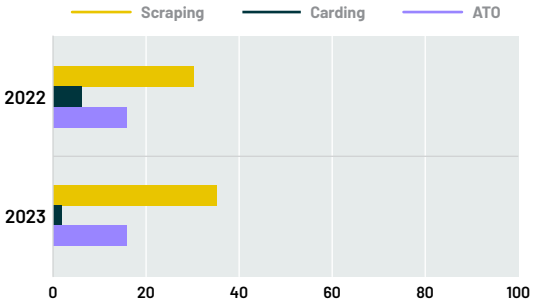
Technology, SaaS & Services

Tech businesses, like the streaming and media businesses above, have a wide variety of potential cybersecurity threats:

- Account takeover attacks (to drain account balances, collect PII, or steal loyalty points)
- Client-side attacks (to collect PII)
- Carding attacks (to test stolen cards with immediate feedback)
- Fake account attacks (chaining fake accounts to exploit new user discounts)

This is a particularly broad bucket, but the delivery mechanism for companies in this category makes it an effective way to group. Depending on the nature of the service being offered, companies in this category may find themselves particularly concerned about account takeover attacks and transaction abuse.

Technology, SaaS & Services Attack Rates – 2022 vs. 2023



PERCENTAGE OF WEB TRAFFIC ATTEMPTING ATTACKS

Account takeover attacks were roughly even across this category over the past year, at **15%** of traffic to login pages. Transaction abuse fell from **6% to 2%**, and web scraping attacks rose year over year, from **30% to 36%**.

5.

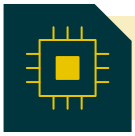
Cybersecurity Trends

In addition to exploring the data from a threat perspective and from an industry perspective, we thought it might be worthwhile to look at some big questions that span multiple industries or attack types and uncover what the Human Defense Platform and Satori Threat Intelligence team can tell us about their impact on the internet today.

Questions like:

- What is the role of AI in uncovering (or perpetrating) attacks? Is AI an attack surface unto itself?
- Loyalty and incentive programs are a crucial lead-generation mechanism for many businesses; are threat actors focusing on those programs for their attacks?
- With so many devices connected to the internet now, are threat actors looking to Internet of Things devices as a source of IP addresses for botnets?

All of these topics will influence threats and threat management in the years to come, as tools for cybersecurity professionals (or for threat actors) or as targets for threat actors to levy attacks on.



Artificial Intelligence

Loyalty & Incentive Programs

Internet of Things

Artificial Intelligence

One of the biggest tech developments of 2023 was the increased access to and awareness of large language models (what most of us think of when we hear "AI"). User-friendly LLMs like **ChatGPT** — a chatbot powered by the OpenAI GPT project — make it possible for non-experts to engage with AI for the first time. Many readers will have opened a ChatGPT or other chatbot window simply to play around with the tools, see what it knew and could tell us.

We're still, as a society, working out what sorts of attacks AI might be able to help facilitate. Can LLMs write the code for account takeover attacks if fed the right parameters to avoid developers' attempts to prevent it? Could they decrypt hashed passwords if fed a leaked list, enabling an attack? Hackers are clever; if they weren't, they wouldn't last very long as hackers.

Many industries have expressed concerns about the ways in which AI might supplant traditional, human-led content creation. AI-generated content is created and packaged in minutes, compared to the days or months it might take a human to write and produce a work of the same length.

What feeds the beast, however, is human-driven. It's content that's been scraped from throughout the web and passed into an LLM to internalize and recapitulate. That content may well be under trademark or copyright protection, which the LLM may not know before it churns out a sequel or screenplay. IP theft — based on AI processing of scraped work — is a potential attack vector for 2024 and beyond.

Spotting AI

In our earlier section on web scraping, we described how a web crawler's user-agent self-declares when it arrives on a website. Large language models generally do the same.

GPT will identify itself in the user-agent, and those user-agents are available on the OpenAI website, along with a collection of IP addresses for cross-reference (or for a webmaster to disallow GPT crawling portions of the website). **Google Gemini** uses the same Googlebot string in the user-agent as Google's main web crawlers. **Claude** lists all of its headers in a Git repo.

The challenge is when you get past the big, familiar names. After that point, the user-agents associated with the crawlers powering the LLMs may not self-declare, or may not do so in an obvious way.

The Human Defense Platform allows customers to allowlist or blocklist known LLM user-agents depending on whether they perceive LLMs crawling their website to be a net benefit or a net detriment. Interestingly, the split is pretty stark, with **80%** of companies making a choice about LLMs opting to block outright and **20%** of companies opting to allow (some companies, however, have taken no explicit position on LLM traffic).

Other threats incorporating AI have already been witnessed in the wild.

"We've found a few examples of AI being used for password guesstimation," said Aviad Kaiserman, Threat Intelligence Analyst. "An attacker feeds a LLM a username or email address, the bot searches for it in databases of compromised credentials, and then tries to figure out what a new password might be based on patterns in old ones."

It's essentially AI-assisted credential cracking. But Kaiserman also spoke of the role AI might play in arming content manipulation.

"In the past, attackers have attempted content manipulation / disinformation campaigns by coming up with the messages themselves and assigning them to the bots for comments," he said. "We expect that attackers will begin using LLMs to generate these messages. This could affect news sites, social media, review and ratings sites, streaming services, essentially anything where user-generated content has an impact on future business."

And this doesn't even take into account the idea that LLMs could become an attack surface unto itself. Could a threat actor coerce concessions from a company chatbot? Or could a threat actor poison a LLM, resulting in inaccurate answers or insights presented not just to the poisoner but to everybody interacting with it?

It's too early to answer these questions, but LLMs and AI are a particular area of interest for HUMAN and the Satori Threat Intelligence team for 2024 and beyond.

Loyalty & Incentive Programs

In our earlier section on account takeover attacks and account fraud, we described loyalty programs as a potential goal for threat actors. Points earned through loyalty programs constitute a pseudo-currency, one that has real-world value, but is limited in its applicability.

But while you can't generally use loyalty points from one business on another business' goods, you also don't need to have a real bank account or an ID to own them. And many loyalty programs have fairly easy setups to transfer points from one account to another.

Kaiserman, a HUMAN Threat Intelligence Analyst, described the mechanism that helps hide the identity of a threat actor in a loyalty point-centric account takeover.

"Successful account takeover attacks lead an attacker to have full access to a cracked account," Kaiserman said. "That includes all of the funds and balances associated with the account, including reward programs. An attacker can harvest these and transfer them to their own account, usually by sending through multiple middleman accounts, which are described in the field as 'mule accounts.'"

HUMAN will publish ***new quantitative and qualitative research*** *about loyalty and incentive program abuse later in 2024.*

Internet of Things

It wasn't all that long ago that the list of devices in your home with an associated IP address could be counted on one hand, maybe two. Laptops, cellphones, maybe a tablet or an early-generation DVR, and that was pretty much it.

In recent years, however, the collection of internet-enabled devices has bloomed dramatically. Refrigerators, doorbells, lamps, connected home hubs, everything talks to the internet now. And everything that does so requires an IP address, often shared among all the devices — smart or not — in a home.

So in the event a smart refrigerator were infected with malware, blocking that traffic isn't as simple as blocking the IP address, because all of the other devices in the home might get caught up in the dragnet. Protecting IoT devices from threats can't rely on IPs as a result. What's more, user-agents can be spoofed; indeed, that's a common tactic of threat actors (though not one that gets past the Human Defense Platform).

What HUMAN researchers are intrigued by is how threat actors who take aim at IoT look at operating systems. There's not a lot of OS to exploit — IoT devices tend to run on/with very simple, lightweight operating systems — and getting malware onto those devices in the first place is hard when there's not a ton of internet activity happening.

IoT has loomed as a potential major threat for a long time. The Mirai botnet demonstrated IoT's capability as a source of devices for bots, and the Satori Threat Intelligence team is actively monitoring for IoT-borne threats as the population of devices continues to grow.

*In recent years the collection of internet-enabled devices has **bloomed dramatically**.*

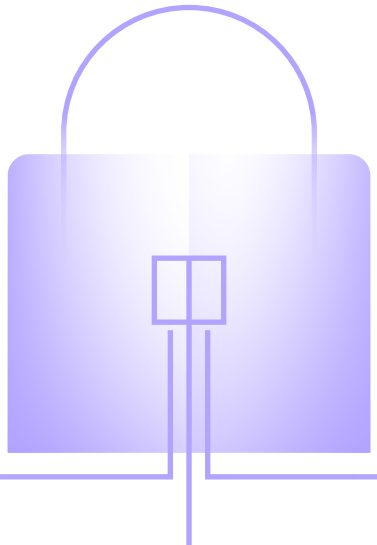
6.

Conclusions & Next Steps

Account takeover attacks, fake accounts, carding, scraping... all of these remain clear and present threats to businesses. HUMAN researchers found that the rate of attacks remained high year over year, but new and emerging tactics incorporating AI may take these threats in new directions in 2024 and beyond.

It's not as dire as the data and anecdotes might make it seem. All of the attacks described were caught and blocked by the Human Defense Platform. No matter how clever threat actors are in their attacks, HUMAN will stop them, and the Satori Threat Intelligence and research teams will find and unravel these threats.

HUMAN uses more than **2,500 individual signals** and more than **300 algorithms** to determine whether an interaction is legitimate or not, protecting websites, mobile apps, and APIs from a broad variety of automated attacks. HUMAN's unmatched visibility into threats across the landscape enables fast and accurate decisioning, ensuring customers protect their users from fraud without any added latency.



Additionally, organizations and end-users can play a part in preventing attacks. Good security hygiene and best practices can significantly reduce the risk of being targeted by an attack, and limit the effectiveness of an attack if one does occur.

Organizations should:

- Enable HTTPS protocols throughout the website, especially within user portals
- Scan for vulnerabilities regularly
- Consider implementing a bug bounty program to identify problems before they're exploited
- Understand all of the microservices and how they interact with data moving through applications
- Review access controls for all employees
- Deploy bot mitigation solution
- Implement client-side protection
- Evaluate account activity post-login

And individual users should:

- Use unique, strong passwords for all logins (password managers can make this easier) and change them periodically
- Ensure software is up-to-date
- Revisit/change passwords on news of a data breach at any organization with which you have an account
- Remain skeptical; if something seems fishy, it probably is

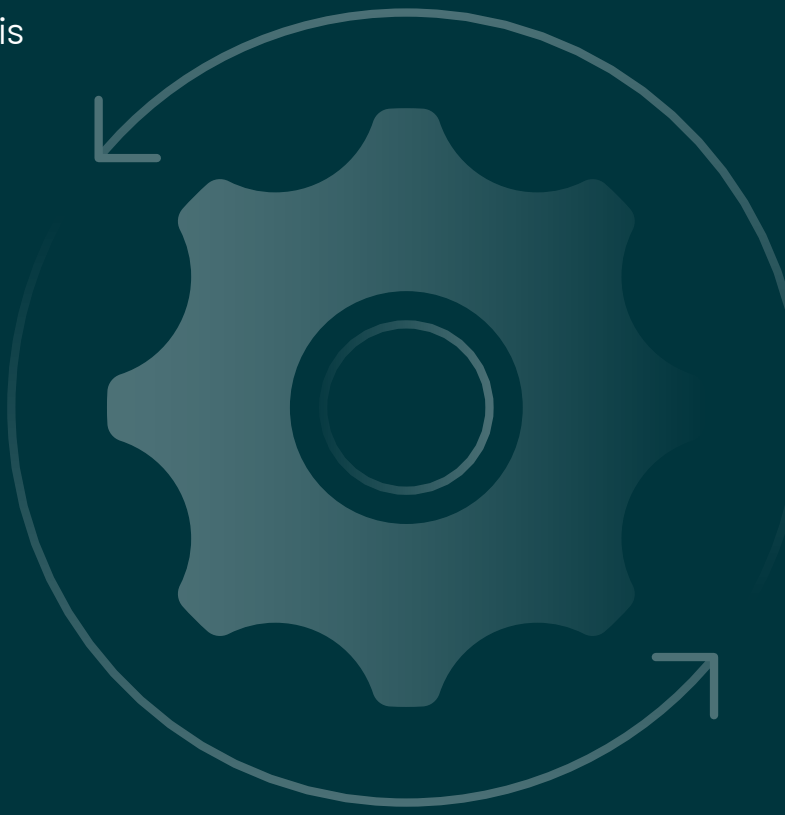
Threat actors aren't going anywhere — as long as there's money changing hands on the internet, cybercriminals will work to steal a piece of it for themselves. The Human Defense Platform protects organizations and users alike, safeguarding the internet for business.

7. Research Methodology

→ The empirical data in this report was drawn from interactions observed by the Human Defense Platform. The insights were derived from HUMAN's cybersecurity clients, which are a subset of the total interactions seen by the Human Defense Platform.

Data in this report has been anonymized to protect privacy.

HUMAN researchers normalized the data in this report to the 75th percentile of customers in the interest of showing a holistic and representative perspective of the attacks observed. In other words, this means outliers and extreme cases have been removed from the data so as not to skew the research.



HUMAN

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit www.humansecurity.com.