NETACEA

REPORT

The Bot Management Review: What are Bots Costing Your Business?

Netacea @Netacea_AI www.netacea.com hello@netacea.com

Contents

Introduction....4

Executive Summary— Bots Cause Real Harm During Pandemic....5

The State of Bot Attacks in a Post-Pandemic World....6

Creating a Common Language: The BLADE® Framework 12

The Financial Impact of Bots....13

How Different Types of Bots are Affecting Different Sectors....16

Conclusion....20

Best Practice Recommendations....21

Bots Glossary....22

Introduction

Pre-pandemic, we thought that we were a digital, tech-savvy society. Lockdown measures showed that we still had some distance to go—and we had to cover that distance quickly. Even people who regularly interacted online had to learn how to do everything online. Businesses were already online to an extent, of course, but this became more than important, and rather vital to survival. This rush was never going to happen without problems.

Some changes as a result of the pandemic are irreversible, in particular the shift to doing business online. In turn, this will change the approaches used by those looking to exploit our habits. There is now plenty opportunity for malicious bots to profit from and wreak havoc on websites, mobile applications, APIs—and the customers who use them.

We know that malicious bots cost businesses millions of dollars every year but quantifying the cost of this activity is challenging. As our research in 2020 discovered, not all businesses were aware of bots and fully understood the threat to their businesses.

This time we wanted to understand more clearly how much bots are costing businesses—and what they are doing to mitigate this cost.

We surveyed 440 businesses based in the USA and UK, across travel, entertainment (including online gaming and streaming), eCommerce, telecommunications and financial services to understand what bots are costing businesses.

The businesses surveyed had turnovers ranging from $350m to over $7bn.

Netacea conducted this survey in collaboration with independent B2B research specialists Coleman Parkes.

Executive summary— Bots cause real harm during pandemic

Over half of all web traffic is made up of automated bots. Half of these bots are malicious and causing real harm to businesses—often to the tune of millions of dollars.

2020 saw every business in every sector rethink how it operates. Some have been more severely hit than others. The travel sector has been amongst those worst affected, but a faltering economy means that even those sectors that might benefit from extended lockdowns—such as online entertainment—are at risk from worries about disposable income.

Unfortunately, the shift to online-first has only encouraged bot operators. In 2020, two-thirds of businesses detected website attacks, just under half had their mobile app attacked, and a quarter—mostly financial services—saw bots attempt to compromise their APIs.

Many businesses are operating at razor-thin margins, and bots are costing them 3.6% of their revenue. For 25% of the businesses we surveyed in this report, that's a quarter of a billion dollars lost.

Our survey also reveals that every sector is facing this problem, though the type of bots and where they are attacking may differ. The biggest problem for most businesses are account checker bots that use breached passwords to take over accounts through credential stuffing, though sniper bots, scalper bots and scraper bots are not too far behind.

One of the biggest surprises is where these attacks originate. Bots, attackers and customers are often from the same parts of the world unlike in, for example, DDoS attacks. Bot operators are perhaps confident that they are unlikely to be detected, and so there is little risk from operating within reach of the authorities.

A common theme concerning the whole cybersecurity industry right now is the length of time between attacks and their discovery. In the case of some high-profile attacks, there have been months between the incident and the realization that something is wrong, meaning hackers may cause damage for all that time. Bot attacks follow this pattern, with around 14 weeks between attack and discovery.

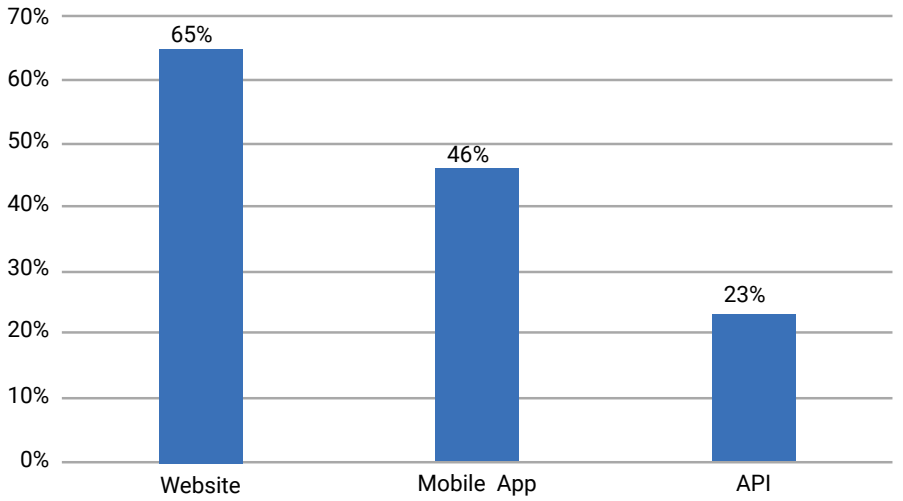
Businesses are aware that bots are a problem and understand the effect they are having on customer satisfaction and their already-squeezed profit margins. The problem they face now is turning this awareness into action. With only 5% of security budgets allocated to the problem, changing this may prove difficult.

The state of bot attacks in a post-pandemic world

The first assumption that we need to test is that, as a result of the pandemic, bot attacks are common and businesses know that they are being attacked. This is undoubtedly true.

Two-thirds of companies identified that their websites had been attacked by bots in 2020, while half detected attacks on their mobile apps and around a quarter discovered a bot attack on their APIs. At least part of this difference can be understood by what different sectors have available as an "attack surface" for bots—streaming services and retailers are less likely to have an exposed API than financial services. There are also the capabilities of bots to consider—far more are designed to exploit websites than mobile apps or APIs.

We suspect that there are many attacks that go unnoticed, but every sector is slowly becoming more educated about the bot threat, and this level of awareness is encouraging. For example, our research from 2020 showed that API attacks were not being taken seriously by any sector, not even financial services. This is changing.

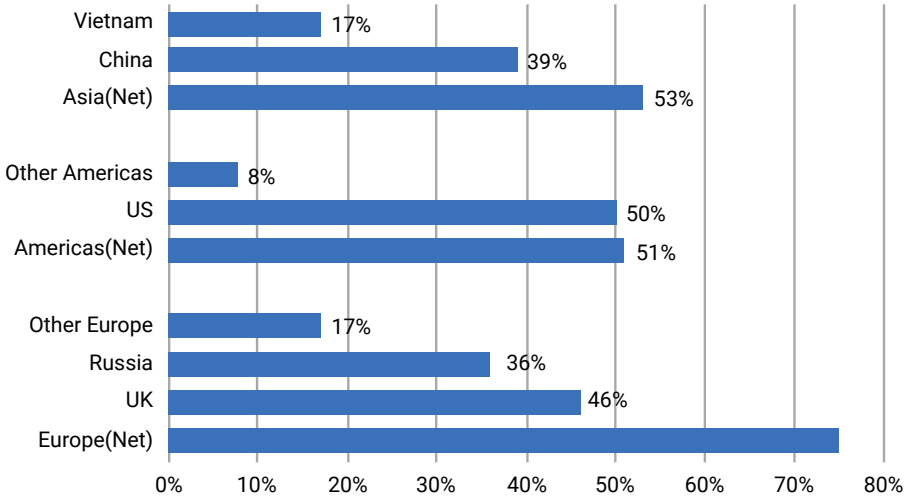


Q1. To your knowledge, which of the following have been attacked by a bot in 2020?

We also wanted to know where these attacks are coming from.

When asked if they knew where these attacks originate, Europe was the most common answer at 75%, followed by Asia (53%) and the Americas (51%). Of those European attacks, 46% said they came from the UK. More businesses were able to identify attacks from the UK or US than attacks from Russia and China.

We shouldn't completely ignore the threat from these countries, but it's important that businesses realize that the threat doesn't always come from foreign actors. We're used to seeing certain countries blamed for cyber-attacks, whether it's hacker groups using ransomware to make money or massive DDoS attacks blamed on nation states. Bots are different. The attacks regularly originate from the same place as the business being attacked, suggesting that the attackers feel comfortable they won't be traced. Not all bot activity is illegal, of course—sniper and scalper bots may affect reputations and be against the terms and conditions of a website, but no crime is necessarily being committed. While proxies may be used to hide the true origin, bot attacks are generally not from countries where attackers can hide, but more likely to be from the same country as the targeted business.



Q2. Do you know where these attacks originate?

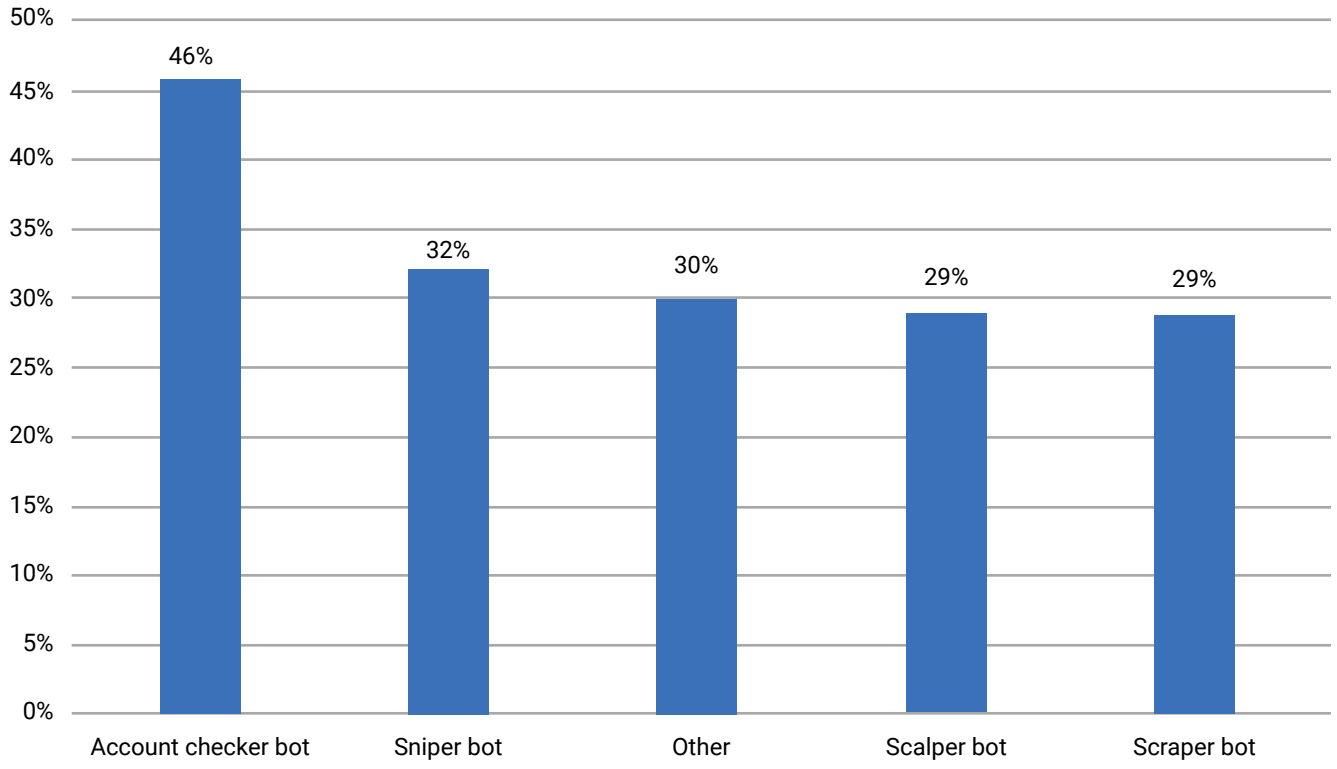
Around a third of businesses could identify attacks from sniper bots (32%), scalper bots (29%), scraper bots (29%) and what we've named "other bots" (30%). Most of the attacks in this latter category were DDoS attacks. There is a strong possibility that these were not deliberate DDoS attacks but lots of people using bots at the same time—a few hundred bot operators trying to snag the latest console could easily overwhelm a site with so many requests at once.

By far the most common bots detected are "account checker" bots. Bot operators take username and password details that have been leaked in data breaches, and check to see if they work elsewhere in a "credential stuffing" attack. As many people reuse the same password, many accounts are taken over in this way. A leak on a discussion forum on one site could, for example, lead to streaming service accounts being taken over.

These accounts can then be resold on a dark web market for a fraction of the cost of a standard account.

That account checker bots are so common points to them being a lucrative business. Big data breaches make the news so often now that they are barely news, and turning this data into profit takes a little effort.

These attacks are concerning, but there's another worrying pattern in cybersecurity we wanted to explore. Attacks first launched in 2020 went undiscovered for months, possibly the best part of a year. Are bot attacks going undiscovered for similar periods?



Q3. What type of bots has your company been attacked by?

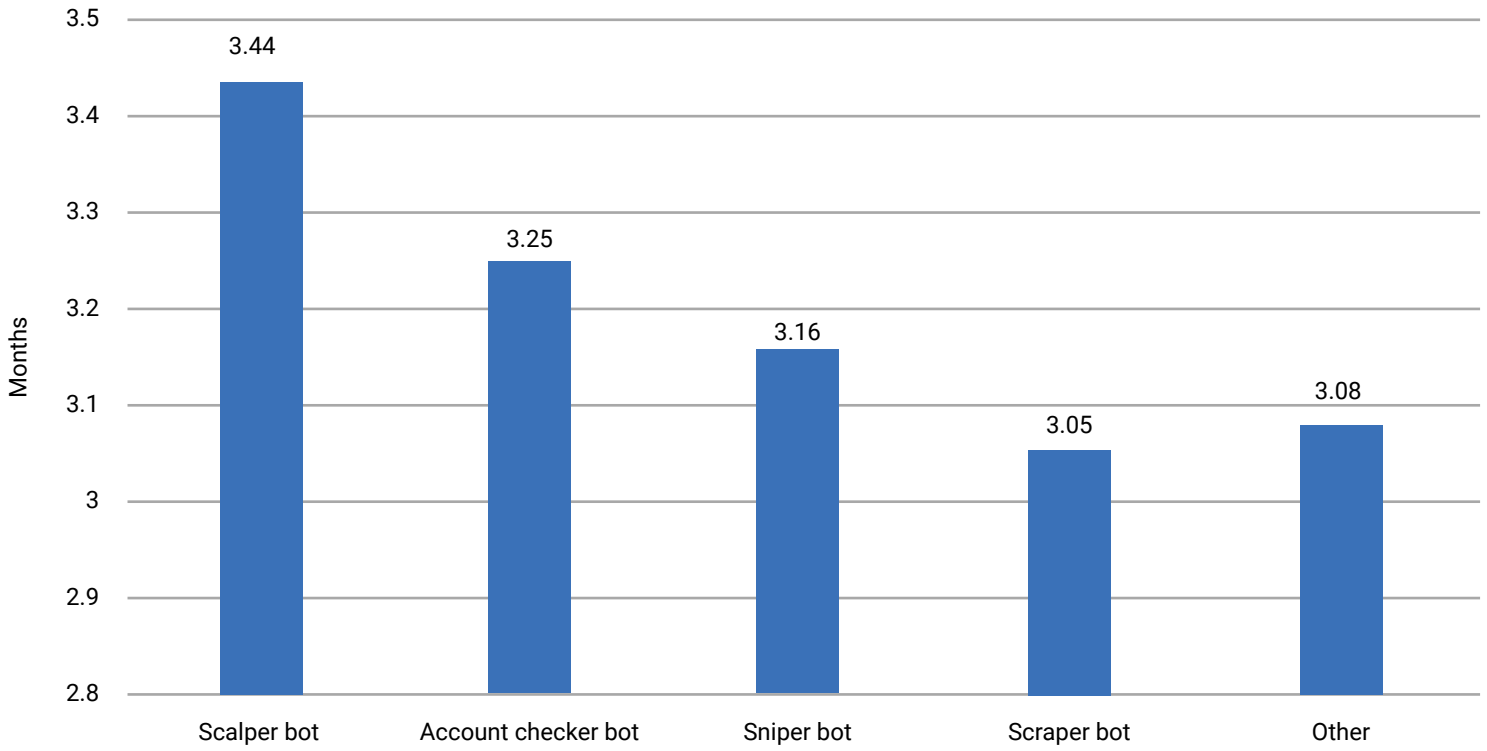
While some types of attack were identified quicker than others, bot attacks took an average of three months to be identified. The bot attacks that took the longest to identify were from scalper bots followed by account checker bots and sniper bots. The most common attack, the account checker bot, took on average 3.25 months—more than 14 weeks—to discover. The nature of these attacks means that the damage will have already been done well before anyone from the target business knows about it.

Why is this? Bot attacks are understood, they are being detected, and their point of origin identified. But it's taking too long for this detection to be put to use, to stop these attacks.

This also suggests that what respondents claim to be DDoS attacks are, in fact, large numbers of bot attacks not intended to bring the site down.

To be effective, genuine DDoS attacks need to be instantly recognized as such and will often be followed by a ransom demand.

We believe that this failure to detect and stop attacks is due, at least in part, to the lack of a unified approach and shared language in the bot community and a lack of understanding around the methods and motivations behind bot attacks. The absence of methodology and framework has left the door open for threat actors to continue to carry out attacks. As long as this problem remains, bots and their operators will have the upper hand.



Q4. How long did it take for your company to realize there had been an attack?

Creating a common language: The BLADE® Framework

Bot mitigation isn't just about building the software that can learn the difference between a real person and an automated bot with malicious intent. We need to create a way of talking about bots that means we can better understand how they work—a common language that enables the cybersecurity industry and its customers to effectively communicate.

To help companies detect bot attacks early and put a stop to bot activity before fraudulent activity can take place, we've created the world's first bot management open-source framework, the Business Logic Attack Definition (The Blade Framework®), which provides a standard approach to combatting malicious bot attacks across a broad range of industries.

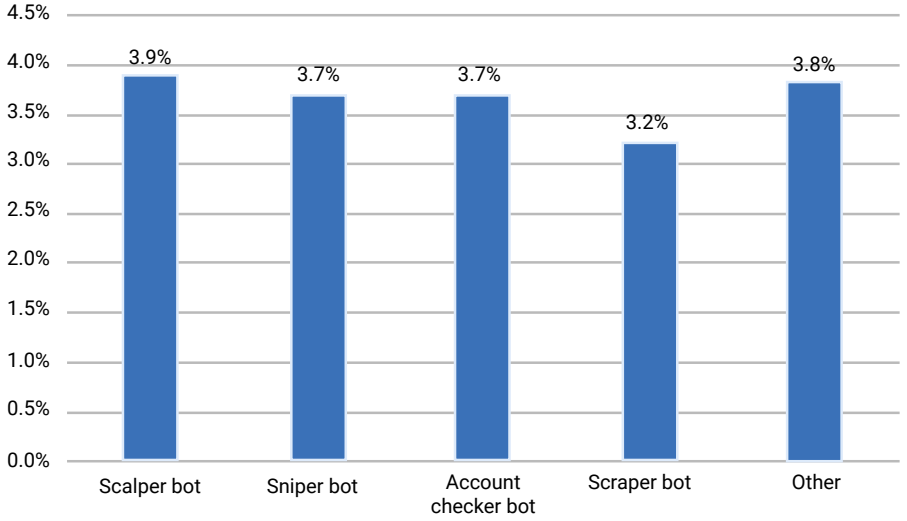
Our aim is for this to be a community-owned asset that will grow and evolve with input from cybersecurity experts and industry influencers from across the globe. More information is available at www.bladeframework.org/.

The financial impact of bots

Bots are more than an inconvenience. They cause real harm to businesses—taking up website resources and slowing them down, skewing analytics, and harming a business's reputation by, for example, buying limited edition goods before genuine customers can get to them. But what about the financial impact?

This is a complex question. Some have a greater, and more clear-cut financial impact, while others are more challenging to accurately link to financial loss. Sales lost to competitors, the cost of website downtime, consumption of web-facing infrastructure, and time spent solving problems in the aftermath of an attack are all partly attributable to bots. There is also the cost of compensating customers who have had loyalty points stolen or had their accounts and credit cards used to buy goods. Even if this is down to poor security hygiene on their part, businesses will often choose to maintain customer goodwill and take the loss. Some bots are even specifically designed to extract Personally Identifiable Information (PII) from customer accounts, and the theft of such PII can, in certain jurisdictions, lead to significant fines under data protection laws (such as the GDPR).

We asked businesses to simply estimate how much bots had cost them as a percentage of online revenue.



Q5. Can you estimate how much bot attacks have cost you as a percentage of online revenue?

Our survey shows that bot attacks cost companies on average, 3.6% of their organization's total online revenue in 2020. This number has to be understood in the context of a year when profit margins narrowed for many businesses. It is not a small number. Far from it—for a quarter of our respondents, who declared an annual turnover in excess of $7 billion, that amounts to at least a quarter of a billion dollars (or £180m).

Bots are having a negative effect on the bottom line of businesses that are already struggling. This is not a minor inconvenience; it is a problem that cannot be ignored

Scalper bots were the biggest cost to companies, with an average loss of 3.9% of online revenue, slightly ahead of sniper bots (3.7%) and account checker bots (3.7%).

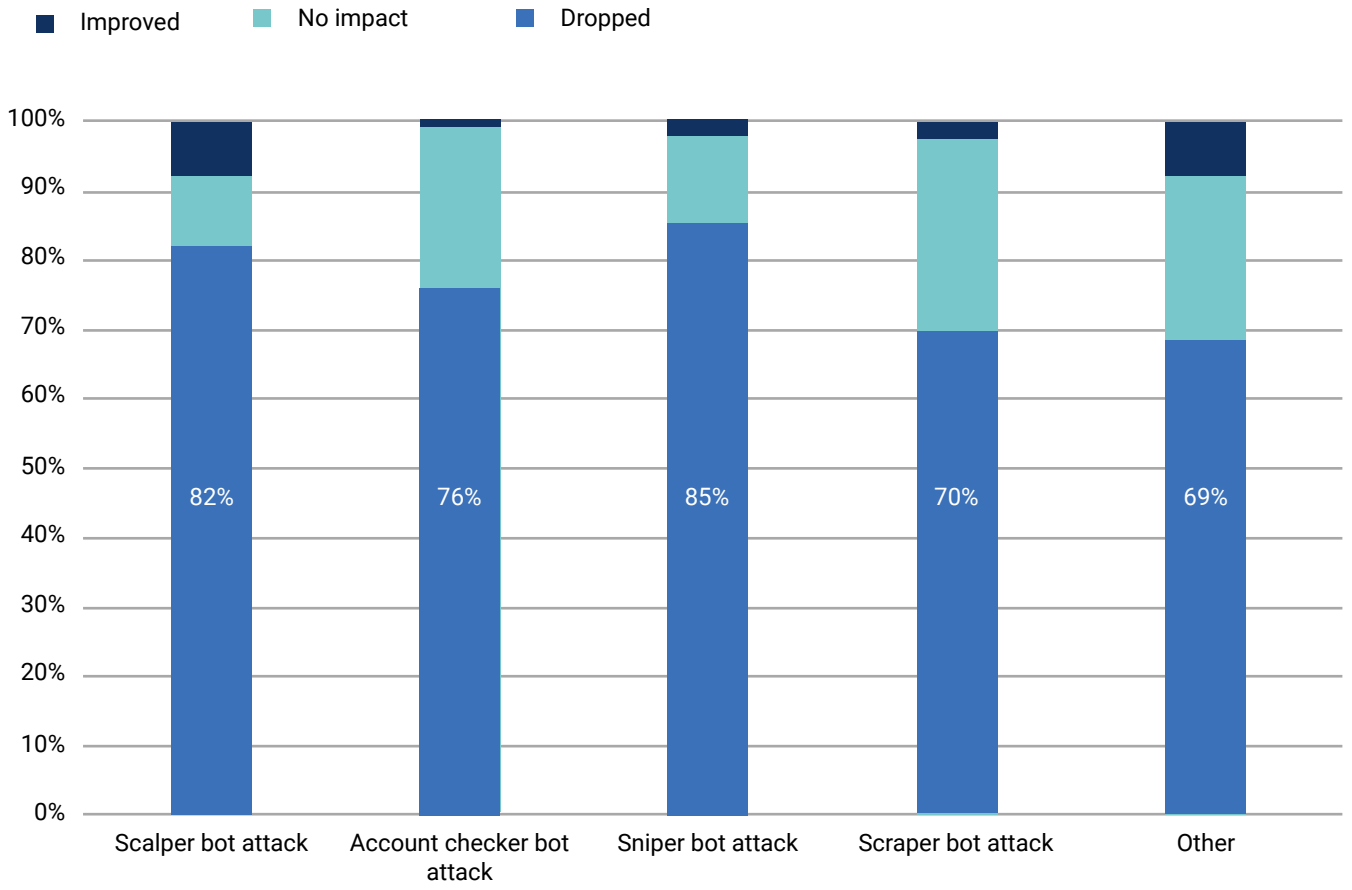
Scalper bots are especially frustrating for customers—more than six months on from release, PlayStation 5 restocks were still headline news on specialist news sites, as bots and customers tried to be the first to buy up limited stock. High-profile bot attacks, and the frustration they cause, have the potential to damage a retailer's reputation. Why would a customer buy from a retailer if they feel continually let down by the digital equivalent of empty shelves?

While this is a big problem, businesses do at least seem to understand that these bots are damaging their bottom line as bad experiences damage their reputation. This is the topic we turn to next.

Bot attacks are not only chipping away at revenue but at customer satisfaction too. An overwhelming number of companies, over 80%, reported that their customer satisfaction had dropped by 5% due to sniper bot and scalper bot attacks. All other types of bots—account checker bots (76%), scraper bots (70%) and other bots (69%)--also had high impacts. Every type of bot was reducing customer satisfaction for at least two thirds of businesses affected. When it comes to customer satisfaction, there is no such thing as a benign bot attack.

These effects are incredibly difficult to quantify. No customer will report that their experience is being made worse by bots, but will instead say that the website was slow or they were unable to buy what they wanted. But these experiences all affect the bottom line. Again, with scalper bots and sniper bots in particular, it's important to remember that an item selling out may not automatically lead to customer satisfaction—inventory being snapped up in a few hours is cause for celebration, but if it happens in seconds, it could be a worry.

Bot mitigation has the possibility of being a differentiator. Respondents report that they have lost business to their competitors due to bots, with 80% of companies seeing between 4% and 5% of their business moving elsewhere. This is unsustainable at a time when growth is necessary to balance a year when staying still was the best many could hope for.



Q6. What impact have bot attacks had on your customer satisfaction?

How different types of bots are affecting different sectors

Experience of bot attacks is not universal across every sector, and it's instructive to look at the big differences we were able to identify.

Nearly all companies (96%) within the travel sector and three quarters (75%) of telcos had their website attacked by bots in 2020. Despite the especially tough year that the travel industry had, bot users still found it lucrative to attack them. Meanwhile, in the eCommerce and online gaming sectors, mobile apps were the biggest target.

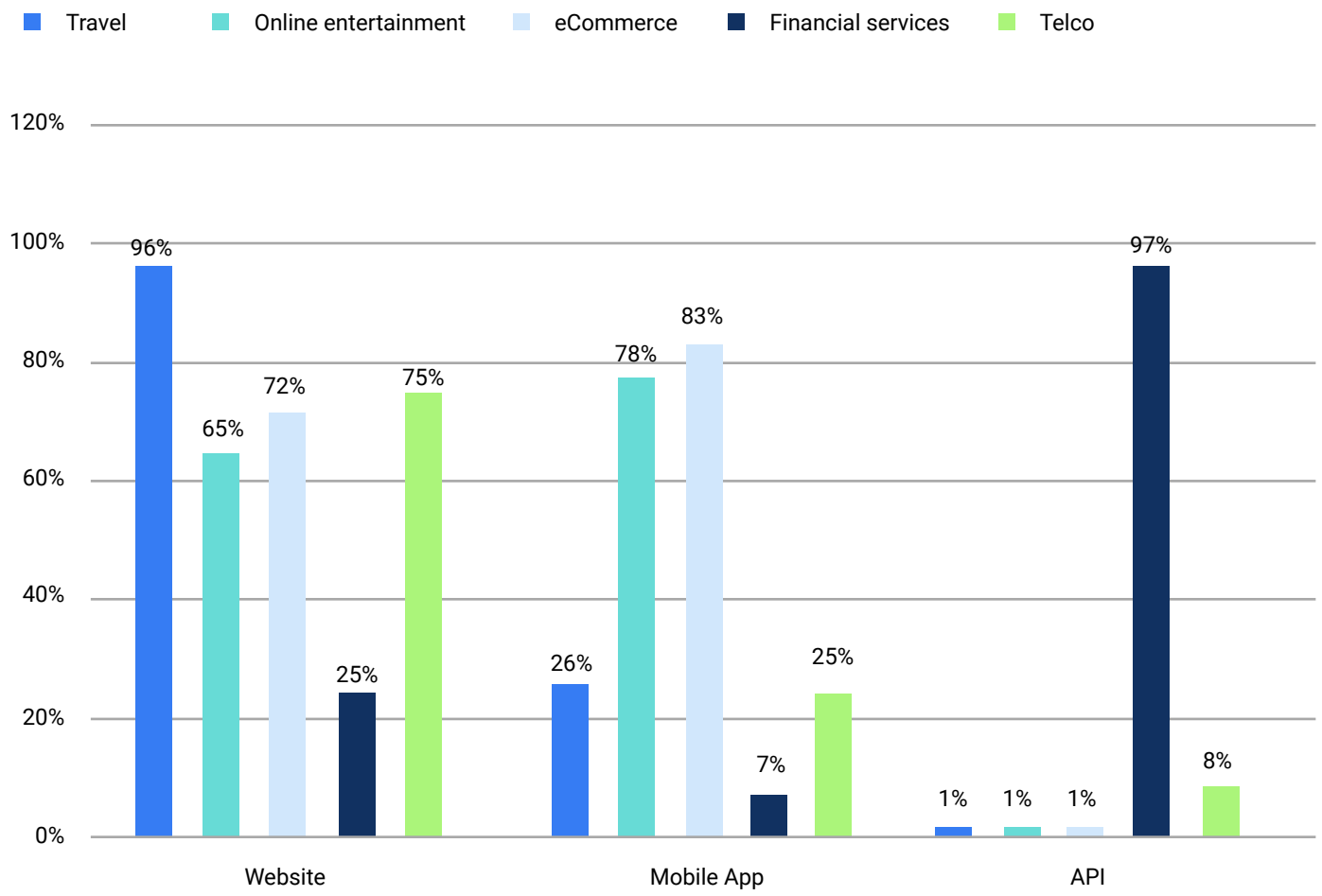
The financial services sector was a completely different story again. Ninety-seven percent of companies reported attacks to their API, whereas just 25% of attacks were against websites and 7% of attacks against mobile apps. In contrast, just 1% of eCommerce and gaming and betting businesses reported attacks to their API.

Why is this so different? It's a combination of available attack surface, and security maturity.

Financial services are highly regulated and need to maintain high levels of security, which makes attacking their websites or mobile apps especially difficult. Their APIs are, by comparison, new and driven by the demands of new regulation—Open Banking and PSD2 laws meant that banks had to create APIs. This is a compelling new target for hackers looking to find a gap in the armor of these security-conscious businesses.

Meanwhile the retail sector reported that mobile apps were under attack more than websites. Retailers have been online for quite some time now and have followed their customers to mobile channels. They have a long history of dealing with bot attacks on websites, perhaps not so much on mobile apps, making them a more attractive attack vector.

Bots will go where there are opportunities for attacks — those businesses that are successfully dealing with website attacks should turn their attention to alternative points of vulnerability, such as their mobile app and API.



Q1a. To your knowledge, which of the following have been attacked by a bot in 2020?

Similarly, we can see some big differences across sectors when it comes to the type of bots being used. Some trends are pretty easy to guess. eCommerce was hit most by scalper bot attacks in 2020—anyone following the news on how games consoles and graphics cards were being snapped up and resold could see this trend in action. Frustrated customers were left paying huge markups for the goods they wanted, bot operators made a tidy profit, and the retailers took a reputational hit.

Meanwhile the financial services sector was under attack from account checker bots, which is understandable given just how lucrative a successful attack could be. The travel and gaming sectors were also hit with account takeover attacks, again because loyalty points and game accounts are so valuable and there are dedicated resale markets for these types of account.

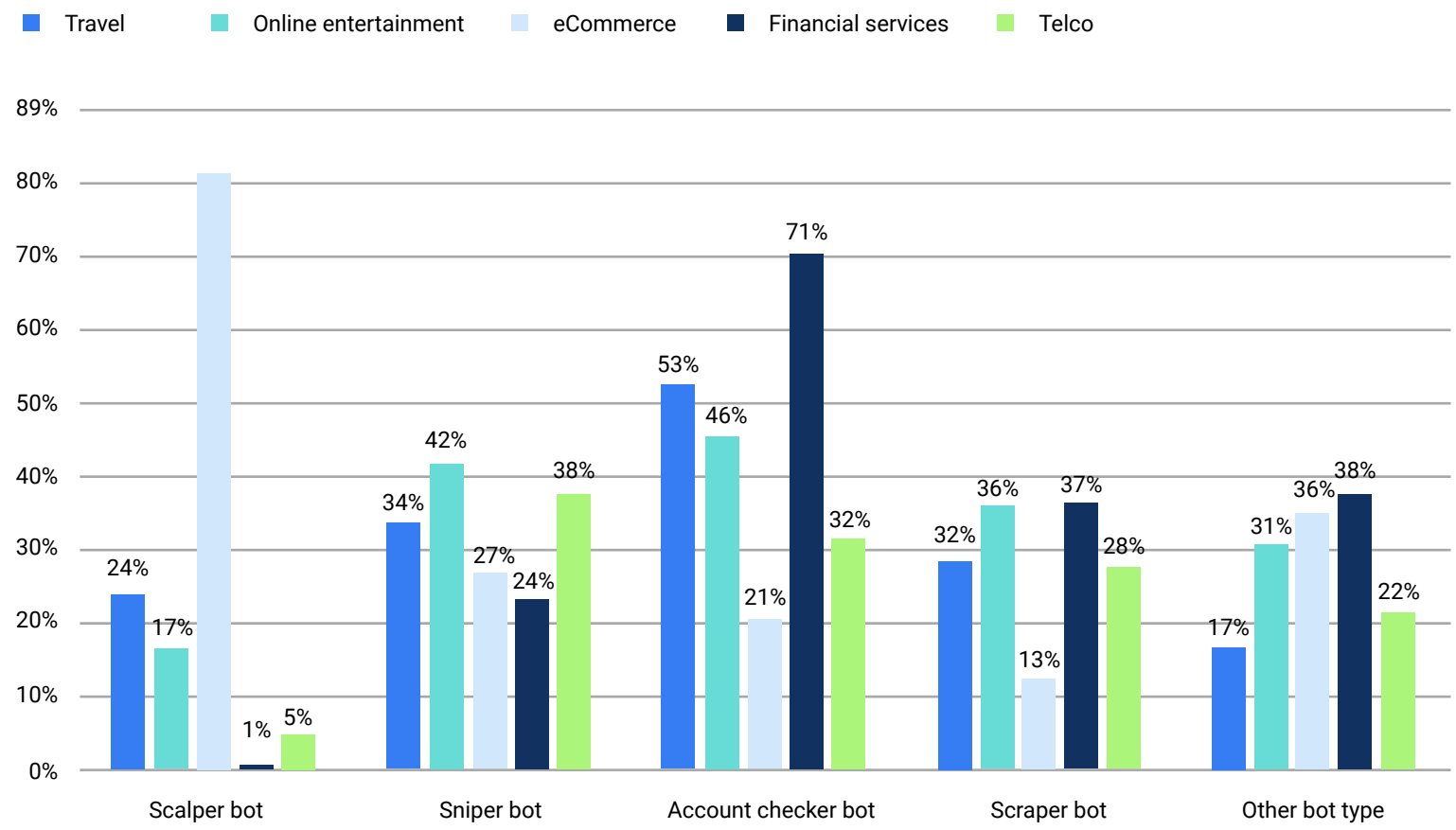
The financial impact of bot attacks also varies across the different sectors surveyed.

Seventy-eight percent of eCommerce businesses stated that scalper bots had a known financial impact in 2020, costing 2-10% of their online revenue. These types of bots also caused customer satisfaction to drop for 79% of eCommerce businesses, and the same businesses estimated they lost up to 10% of their business to competitors as a direct result of this activity.

Businesses from the online gaming and financial services sectors had a similar story to tell when reporting the cost of serving account checker bots. Fifty-nine percent and 69% respectively stated that account takeover bots had a known financial impact in 2020, with 33% and 37% of this number attributing bot activity to losses of 3% of online revenue.

When it comes to the travel sector, 71% of businesses stated sniper bots had a known financial impact in 2020, with 38% of this number attributing bot activity to losses of 4% of online revenue.

Every sector has a bot problem, but each sector is under attack in its own way. This should be reflected in any attempts to fix the problem.



Q 3a. What type of bots have you been affected by? (by sector)

Conclusion

The problem of bots is not one of awareness, at least. Our previous research revealed that businesses may not be aware of the scale of the problem, but here we can see that businesses are aware of the financial impact bot attacks can have, and the effects on customer satisfaction.

Our findings show that businesses are suffering a significant loss of revenue because of bot attacks. This would be concerning in any year, but the tough times businesses have suffered recently make this all the worse. It also demonstrates businesses' limited ability to counteract the problem, most notably showcased by the long period of time taken to identify bot attacks.

So how to fix it? The challenge facing many businesses is acquiring the security budget to identify malicious bot threats quickly and mitigate them before the damage can be done. Our survey reveals companies dedicate on average 5.19% of their overall security budget for bot management. Given the level and impact of attacks this is either insufficient or not being used effectively.

As a proportion of security spend, the amount dedicated to bot mitigation has actually decreased. Given the increased need for security, this is likely simply as a proportion, not in absolute terms. But with bots causing so many issues, it clearly needs greater focus. Businesses with the highest turnover, over $7bn, spent more on bot mitigation as a proportion of their security budgets than others, though we cannot say for sure if this is because they understand the problem better or are simply bigger targets.

That is not to say that the solution is simply to throw money at the problem. Identifying where the bots are attacking, and what bots are creating the biggest problem, is a key first step.

Ultimately, businesses recognize that they are under attack from bots, and understand the effect this is having on their bottom line. The route forward is to turn this understanding into action to prevent and mitigate bot attacks, and prevent this sizable drain on revenue. For many businesses, there are millions of dollars riding on how this problem is tackled.

Best practice recommendations

What practical steps can businesses take to solve the bot problem? At Netacea we look beyond asking humans to prove they are not bots and instead focus on the user's intent; "What is this user doing?"

We take a server-side approach, rather than placing our solution on a client's website, using web log analysis to build a profile of user interactions with a website. With this data we're able to unmask the intent behind user activity, no matter how sophisticated and human-like the user's behavior appears.

Reframing the question to focus on intent means we are inherently focused on rapid and accurate bot mitigation that does not invade a user's privacy.

To find out more about Netacea's unique approach to stopping sophisticated bot threats, visit www.netacea.com/why-netacea or talk to our team today at hello@netacea.com.

We are also committed to changing the conversation around bots, creating a common language and a better understanding of how bot attacks work.

Inspired by MITRE ATT&CK, a curated knowledge base of cybersecurity threats, we have created the The BLADE Framework®, an open-source knowledge base designed to help cybersecurity professionals identify the tactics and techniques used to exploit weaknesses in business logic websites, mobile apps and APIs.

To use a real-world comparison, MITRE ATT&CK describes the equivalent of a gang drilling a tunnel into a bank vault, whereas a business logic attack

would be like the criminals successfully impersonating the banks' customers, making a withdrawal from the bank teller and walking out of the front door with all the gold.

To find out more and to contribute to the project, visit www.bladeframework.org.

Bots glossary

- **Account checker bots** take lists of leaked username and password pairs (aka combo lists) and test them against a website. This is also known as a credential stuffing attack and relies on reused passwords. They will often also try to "brute force" access to accounts by using a known username with common passwords, again taking advantage of poor security hygiene.

- **Sniper bots** monitor time-based activity and submit information at the very last moment, removing the opportunity for other people to respond to that action. Commonly seen on auction sites.

- **Scalper bots** automate the process of buying limited goods, such as event tickets, completing the checkout process in a fraction of the time it would take any legitimate user. Sometimes known as "sneaker bots" and "grinch bots".

- **Scraper bots** are used to collect large amounts of data from websites for use elsewhere. These can be good (comparison sites that drive business) or bad (stealing and republishing content).

- **Other bots** include DDoS attacks, which use a large number of compromised devices (also known as a botnet) to overwhelm a website and knock it offline, carding bots that check stolen card details, ad fraud bots, and inventory hoarding bots (similar to scalper bots but these keep items in baskets to manipulate a site).