NETACEA

REPORT

The Bot Management Review: How businesses are dealing with bot attacks in 2022

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

NETACEA

Contents

NETACEA

Introduction

In 2021, Netacea published its “Cost of Bots” report. We knew bots were a nuisance to both businesses and their customers—buying up stock, sniping auctions, scraping content and so on—but we wanted to know more about the cost to businesses. What could businesses tell us about the revenue they have lost, the effect on their reputation, and the bad decisions based on bad analytics, all due to bots.

Our results were startling. We found that bots were costing businesses around 3.6% of their revenue, potentially enough to mean the difference between profit and loss. We also found that there was a great deal of misunderstanding about the nature of bots and how to prevent attacks—making tackling this problem even more difficult. We found that attacks were focused on websites rather than mobile apps and APIs, or at least, that’s where businesses were detecting them.

2021 was a time of flux, of lockdowns, furloughs, and home working. A lot of predictions were made as to how this would change cybersecurity. There was some evidence that bot use was on the increase, media reports of members of the public buying and reselling goods using bots to make a living, and worries that hybrid working would mean a huge spike in online criminal activity. Was this part of a long-term trend, or just temporary?

So, a year on, we wanted to know what has changed. Has remote working led to a new wave of bot attacks? Is there a better understanding of how these attacks work? Are businesses fighting back, or losing the war?

Netacea conducted this survey in collaboration with independent B2B research specialist Coleman Parkes. The businesses surveyed had turnovers ranging from $350m to over $7bn.

Executive summary

Can we say that businesses are winning the war against bots? Not quite—at least, not yet. But there's a suggestion that the tide is starting to turn.

Many of our findings in this report could be read as a failure of those being attacked to face up to the problem. We think that the opposite is in fact true. A growing understanding and increased investment in bot mitigation means that businesses understand the threat better than ever. As a result, they are uncovering more bot threats and identifying where they are being hit hardest.

There is also a better understanding of where bots can attack. Last year's report showed that bots were focused on websites with only a few attacking APIs and mobile apps. This is shifting, partly due to a better understanding and because businesses are playing whack-a-mole: as they shore up their defences in one place, attackers will look elsewhere. But the fact that businesses are seeing these attacks is reassuring, the first step towards containing them.

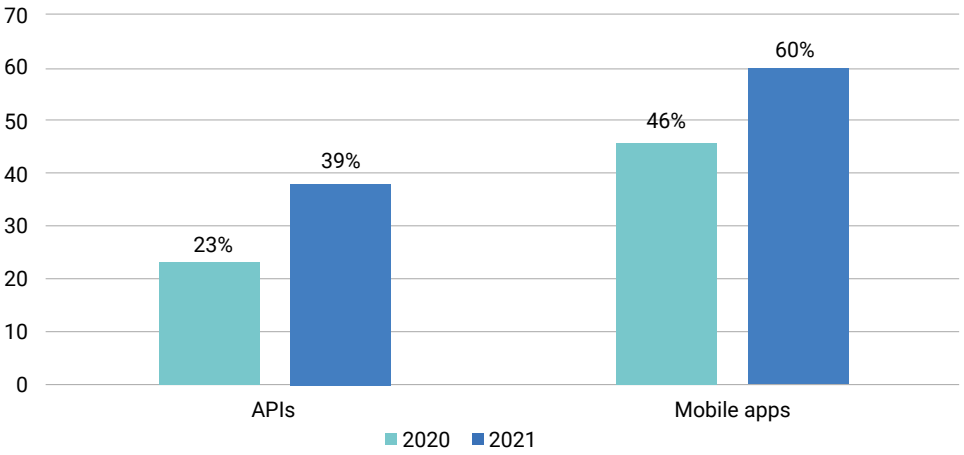
Also encouraging is the news that budgets have increased. Understanding the problem is all very well, but investment is necessary to fix it. Other results, such as an increase in dissatisfied customers and the impact of skewed analytics, can also be explained by better understanding.

But we can't cheer too loudly, not yet. In many ways businesses are not pushing back hard enough, and in others they are losing ground. Bot attacks go undiscovered for an average of 16 weeks, up to two weeks from last year, meaning bots are free to wreak havoc for far too long. And while there are fewer businesses believing myths about bots, far too many still have an incorrect understanding of where attacks come from, how they work, and what can be done to mitigate them.

Overall, this year's results are cause for muted optimism. We are moving in the right direction in the fight against bots. But to win, we need to move faster.

How bot attacks are changing

Q1. To your knowledge, which of the following have been attacked by a bot in your company in 2021?

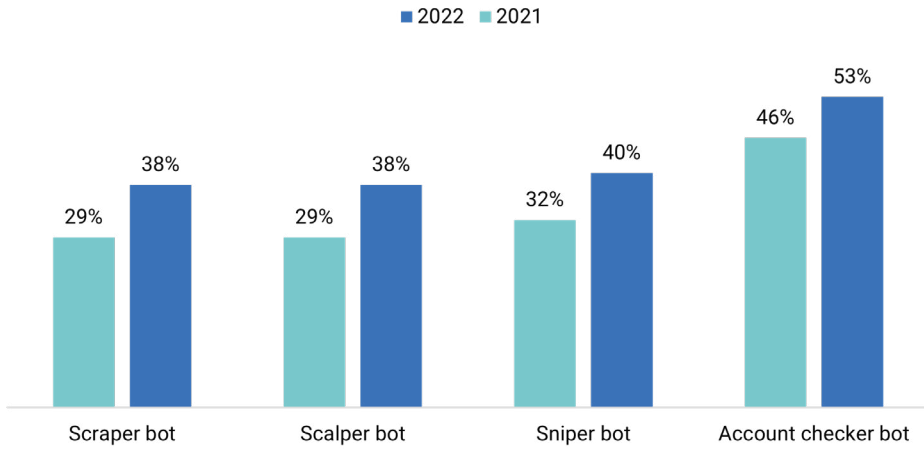


Last year's research report into the cost of bots found that businesses were both vulnerable to, and aware of, the cost of bot attacks to their business. A year later, the landscape looks quite similar, with an increase in the number of attacks. This means two things could be true, that the number of bot attacks has increased, or that a greater awareness of attacks means that more attacks are being uncovered. The reality is likely to be a combination of both.

In response to rising awareness and increased security measures from businesses, we've seen a change in the way that attackers are operating. While it's encouraging to see that attacks on websites have remained static, attacks have increased elsewhere--APIs and mobile apps have both been targeted by bots more this year than last.

The trend is similar across each sector, but there are some notable aspects. Financial services were already suffering attacks to their websites and APIs, but the last year has seen a spike in attacks to mobile apps. However, online retail has seen a marked increase in attacks on APIs, up 21 percentage point from almost nothing. This suggests increased awareness—we simply don't believe that there was so few attacks before.

Not only has there been an increase in attacks, the attacks have increased for the four main bot types over the last year, and "others" has decreased. This suggests increased focus on attacks that have a financial motive.

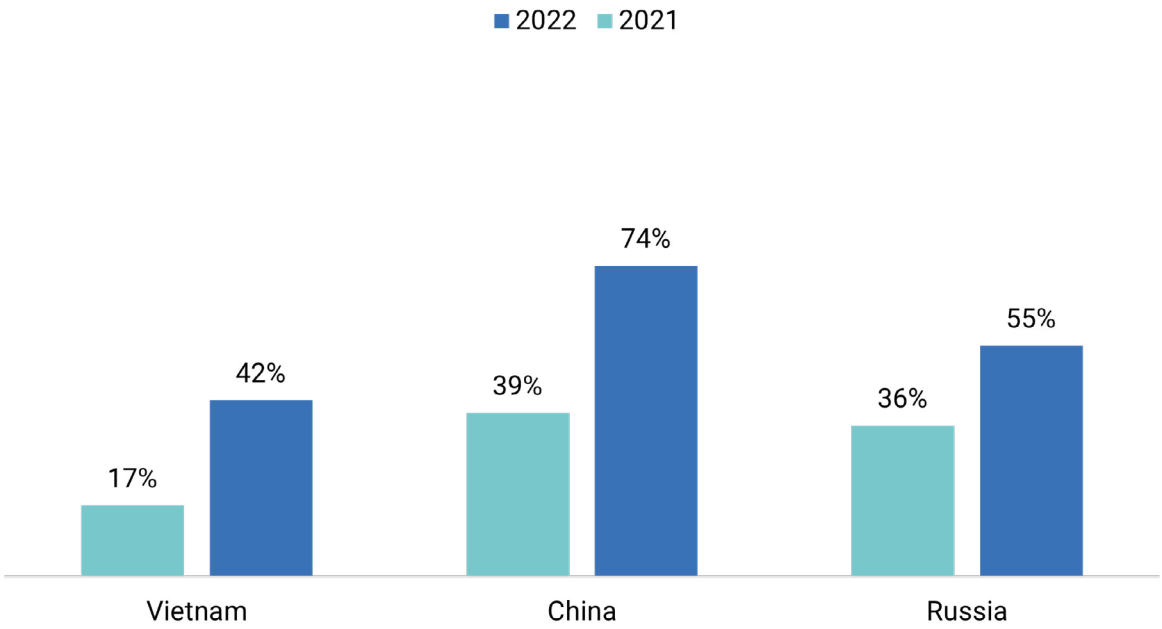


Q2. What type of bots has your company been attacked by in 2021?

When we asked about the origin of these attacks, we found little change in the number of attacks coming from the UK and USA, but attacks from Russia, China and Vietnam have increased sharply.

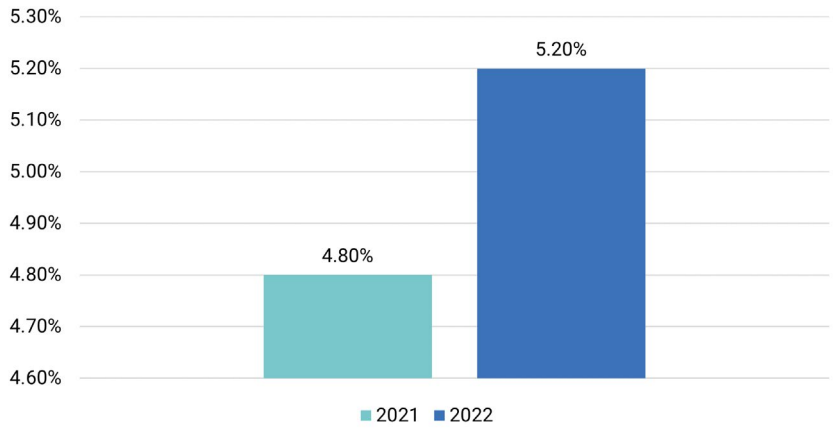
Cyril Noel-Tagoe, Principal Security Researcher at Netacea -

"Due to the ease at which bots can spoof their location through proxy networks, it can be difficult to attribute bot attacks to specific geographies. However, the self reported increase in attacks from these geographies is consistent with what we are seeing. In particular, we've seen a rise in credential stuffing and carding attempts. These types of attacks are relatively low risk monetisation options for cyber criminals, who can resell the validated credentials or payment card details."

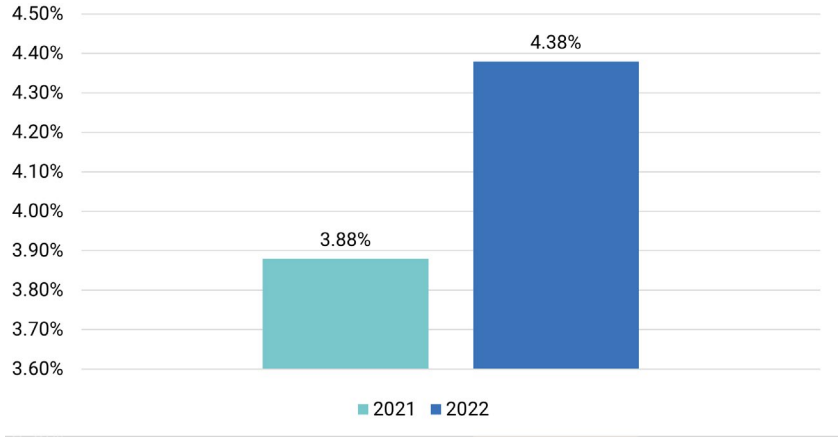


Q3. Do you know which countries these attacks in 2021 have come from?

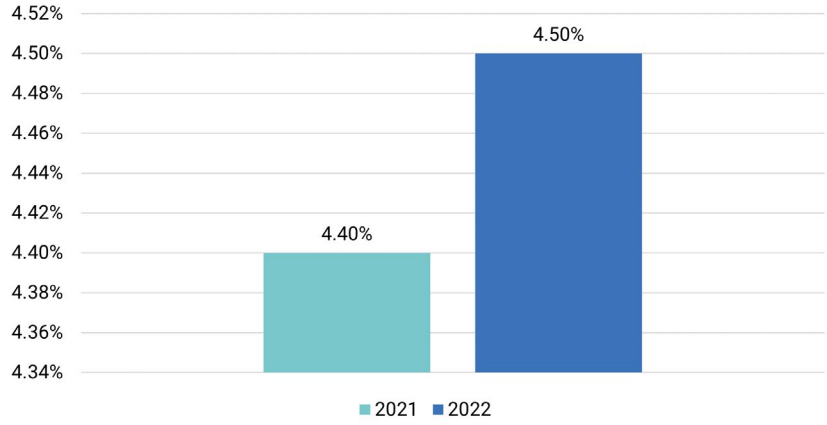
When it comes to the other sectors surveyed, the number of fake telco accounts has remained steady, and there has been a slight decrease in fraudulent streaming and gaming accounts. Credential stuffing accounts are, however, up from last year. There has been a slight shift to stealing genuine accounts rather than creating new fraudulent accounts. If businesses are cracking down on the creation of fraudulent accounts, then this shows how attackers shift their attacks rather than be completely deterred.



Q4. What % of your customer accounts have you identified as being fraudulent and not used by legitimate users in the last 12 months?

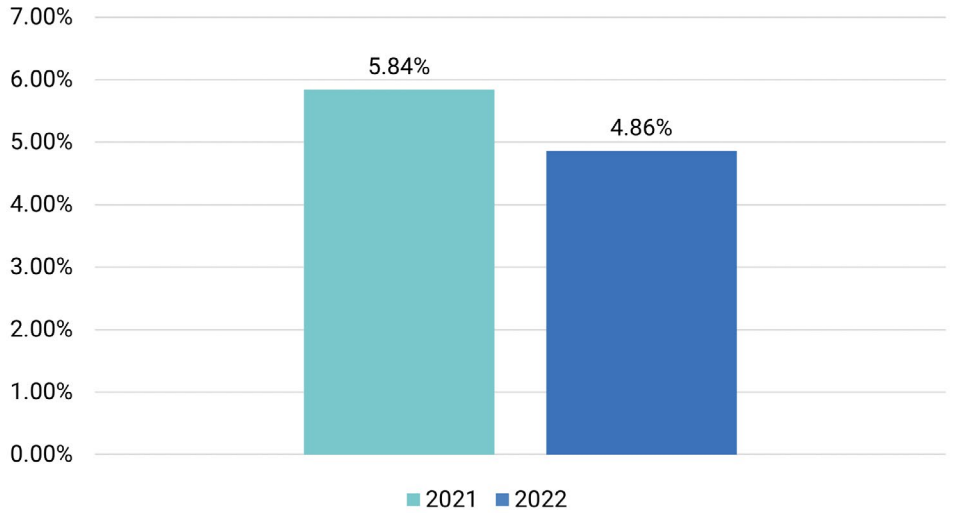


Q6. What % of your customer accounts have been breached as a result of credential stuffing/ card cracking in the last 12 months?

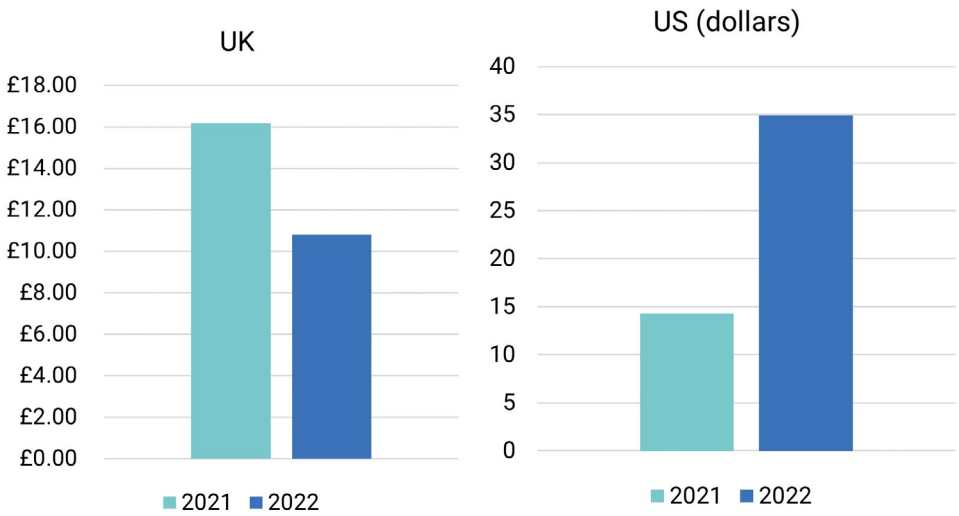


Q5. What % of your new installations have been for fake accounts/customers?

The theft of loyalty points tells a similar story. The percentage of loyalty points being stolen by bots has decreased slightly, but we see a marked difference between the USA and UK. While the UK has seen a fall in the average value of points being stolen, the USA has seen a big increase. Hackers in the USA are being more targeted, seeking out fewer more valuable accounts—when selling these on, these will sell at a greater profit. Again, this is a shift likely brought on by attempts to crack down on hackers. Rather than stop, hackers are stealing fewer accounts for greater reward.



Q7. Please could you estimate what % of loyalty points, if any, were stolen by bots in the last 12 months at your company?

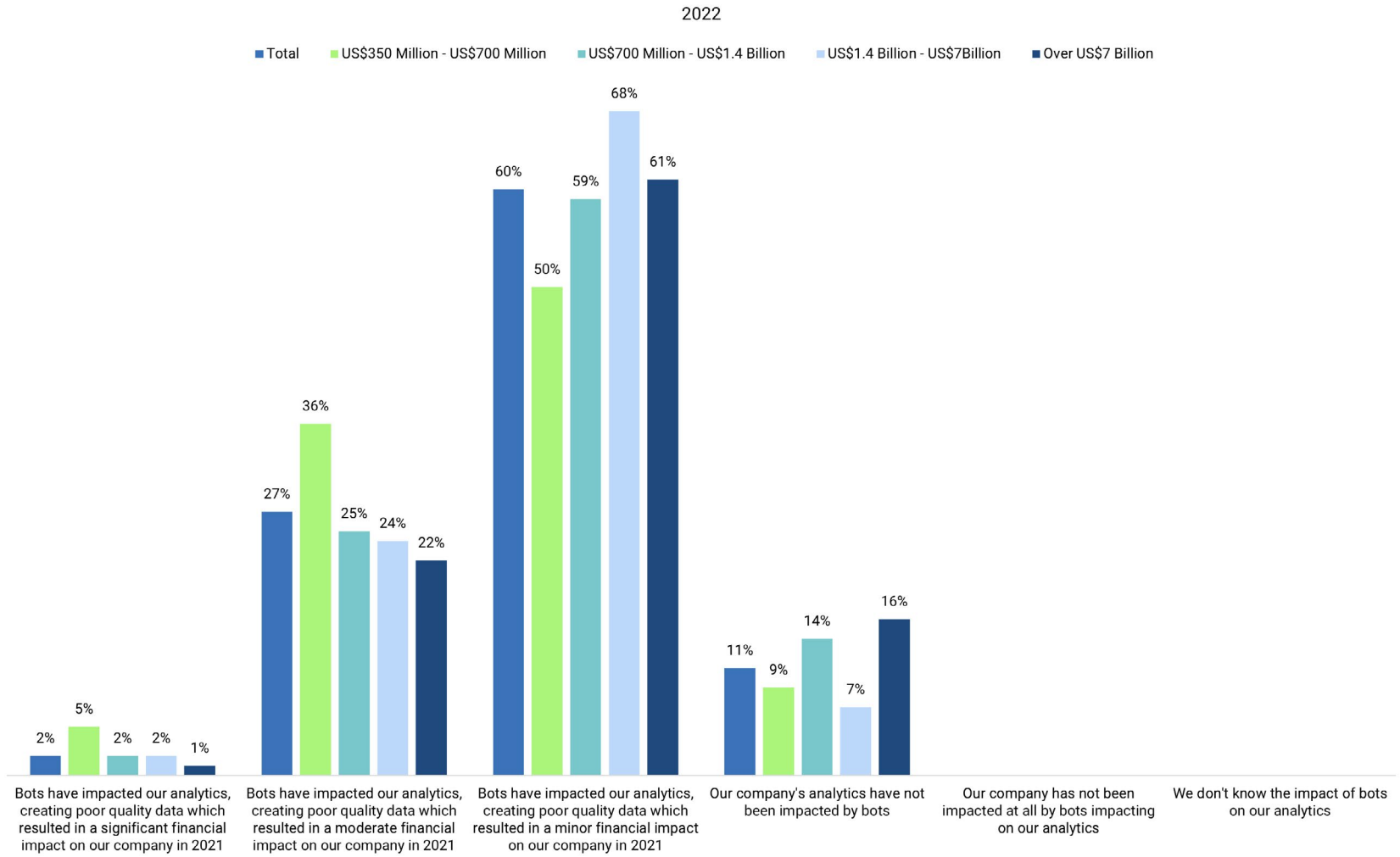


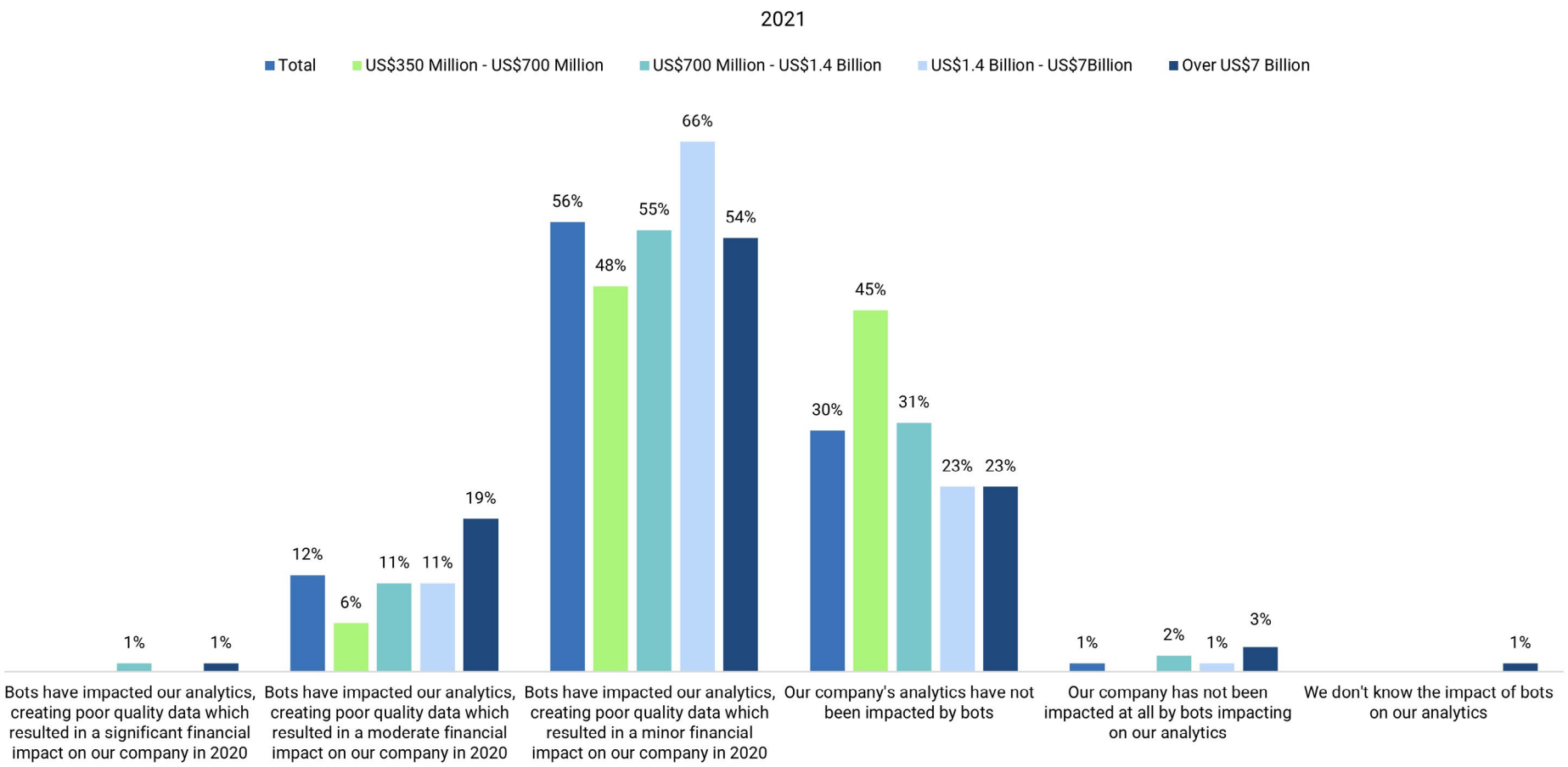
Q8. What was the average value of loyalty points stolen per customer account?

Overall, it would be easy to see changes uncovered here as a regression—bot attacks are more focused, happening more often, and are targeting new areas. But a big part of this is likely to be down to increased awareness of bots, especially those targeting APIs and mobile apps that were previously ignored in some verticals. This is progress, albeit slow.

The cost of skewed analytics

Last year we revealed that businesses were basing at least some of their decisions on false data, that bots visiting websites, pretending to be everyday consumers, were being treated as such. There has been little change in the number of marketing decisions that rely on analytics, so this remains a potential problem.




2021
Total
US$350 Million - US$700 Million
US$700 Million - US$1.4 Billion
US$1.4 Billion - US$7Billion
Over US$7 Billion
1%
1%
12%
6%
11%
11%
19%
56%
48%
55%
66%
54%
30%
45%
31%
23%
23%
1%
2%
1%
3%
1%
Bots have impacted our analytics, creating poor quality data which resulted in a significant financial impact on our company in 2020
Bots have impacted our analytics, creating poor quality data which resulted in a moderate financial impact on our company in 2020
Bots have impacted our analytics, creating poor quality data which resulted in a minor financial impact on our company in 2020
Our company's analytics have not been impacted by bots
Our company has not been impacted at all by bots impacting on our analytics
We don't know the impact of bots on our analytics

There does seem to be some improvement here. There has been a shift from “moderate” to “minor” impact of bots on analytics, and only a handful of those surveyed reporting a major impact. Businesses are fighting back here… to an extent.

The revenue impact, the actual cost of skewed analytics, has increased from 4% to 5%. This seems counterintuitive—how can the impact both decrease and increase at the same time?

As before, this is likely to be down to a better understanding of the problem. More bot attacks are being detected, and factored into decision making, but at the same time businesses better understand the scale of the problem. As before, it doesn’t look like progress, but here businesses seem to be moving in the right direction.

Cyril Noel-Tagoe, Principal Security Researcher at Netacea -

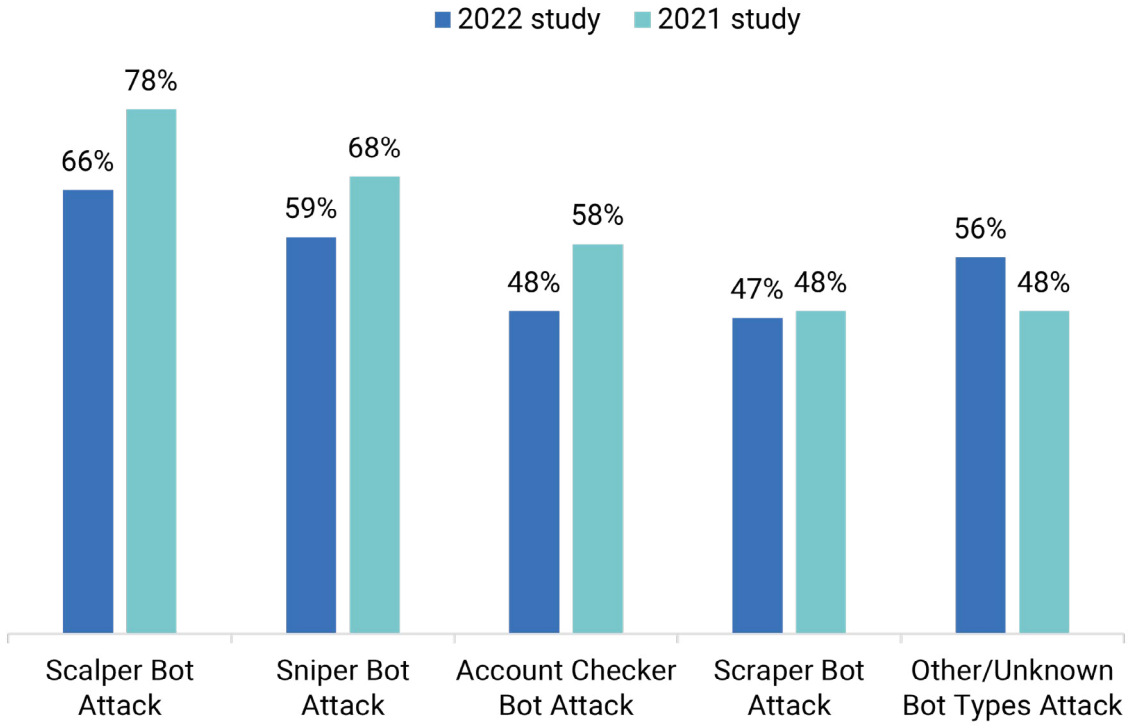
“Businesses are right to pay close attention to their web analytics—the tools we have to interrogate customer journeys can give amazing insights into how customers think and the small changes that can increase sales. Bots do their best to spoil that, skewing analytics and leading businesses into bad decisions. Some businesses have even launched entire marketing campaigns that have been based on the false data created by bots.”

How are businesses reacting?

One of the most concerning developments since our last report is that, despite increased awareness and investment, businesses are taking longer to react to bot attacks than before. In 2021 the average time to react was between 12 and 14 weeks. Now it's closer to 16 weeks.

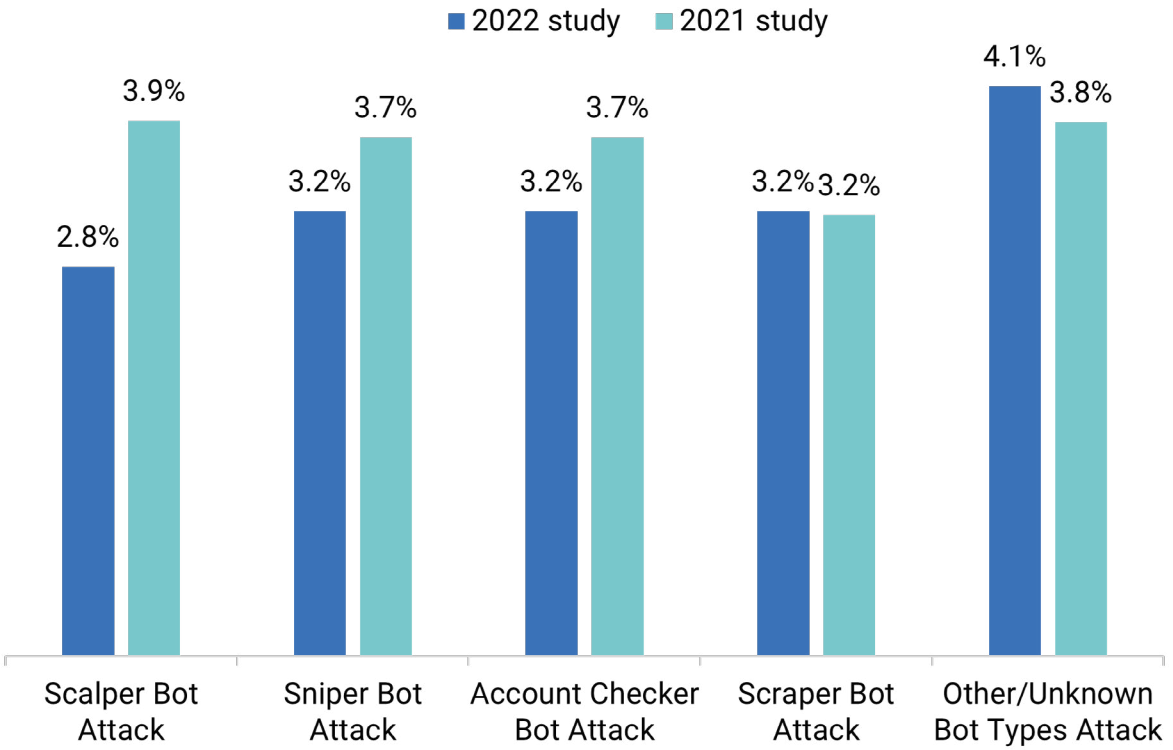
Cyril Noel-Tagoe, Principal Security Researcher at Netacea -

"Bot mitigation can be a bit of a cat and mouse game at times. Whilst businesses are investing in better defences, attackers are developing more advanced bots to evade or bypass those defences. There has been a marked rise in bots hiding behind residential proxies and rotating their user agents and IP addresses, amongst other techniques, to avoid detection. But as businesses improve their defences, they are also catching bots that previously went unnoticed."



Q10. Has this bot type that you have experienced had a known financial impact on your company in terms of revenue lost, cost impact etc. in 2021?

This is the most concerning finding of this report. On average, bots are able to attack websites for around four months before being discovered. While much of this report shows gradual improvement in the fight against bots, this is one area where businesses are regressing. Bot attacks being undiscovered for three months was already unacceptable—few businesses would accept any other kind of attack going unseen for this length of time. Businesses may be discovering more bot attacks, but it must be faster.



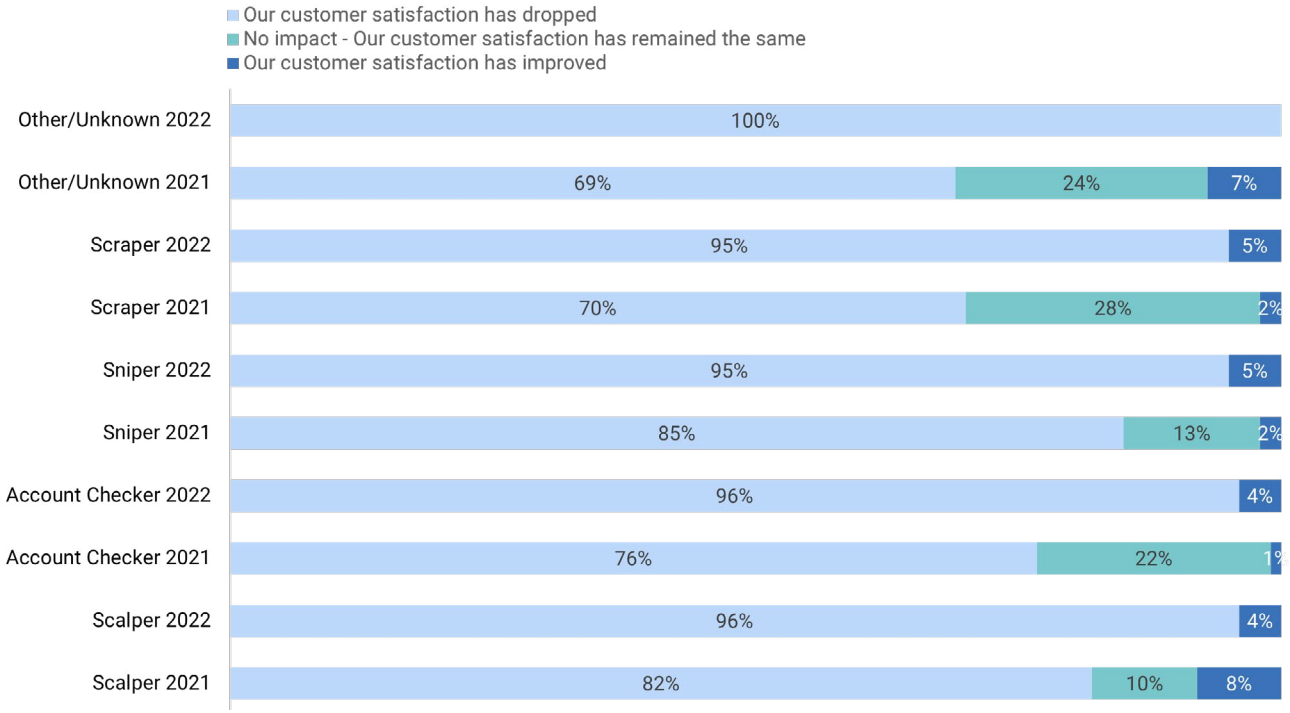
Q11. Please could you estimate how much bot attacks have cost your company as a percentage of your online revenue

Despite this, fewer businesses are taking a financial hit from bot attacks, and those that are suffering estimate that the effect on revenue is slightly down—though still significant. So while more bot attacks are being discovered, this is not leading to a greater financial impact on businesses.

Most notably, the financial impact of scalper bots saw the biggest decrease. As scalper bots were the subject of a great deal of media attention, this makes sense and is welcome news. Businesses that understand the impact of bot attacks are taking steps to mitigate the problem.

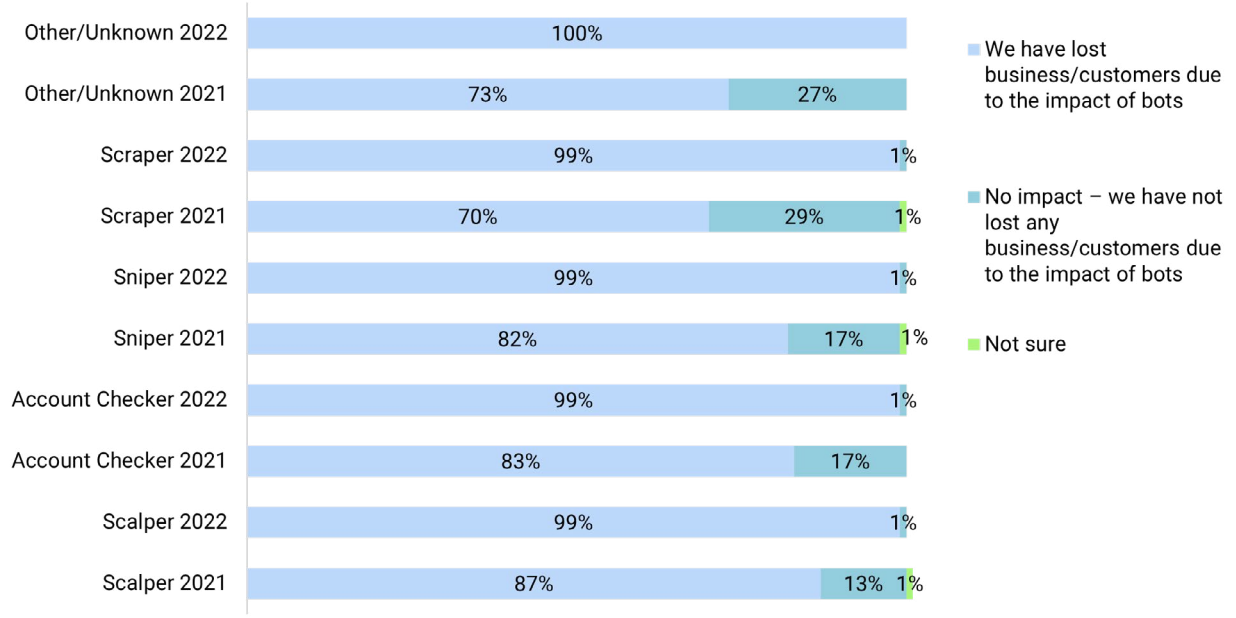
However, the impact is being felt elsewhere. Almost all businesses say that their customer satisfaction has dropped thanks to all types of bot attacks, an increase from 2021.

We see this as, overall, a welcome finding—businesses now understand that bot attacks affect how customers feel about them. This is likely to be a shift in understanding, not in customer satisfaction. Customers were already frustrated by the effects of bot attacks, this just wasn't realised by all. This is backed up by the finding that while businesses realise they are losing customers to bot attacks, they are losing fewer than last year.

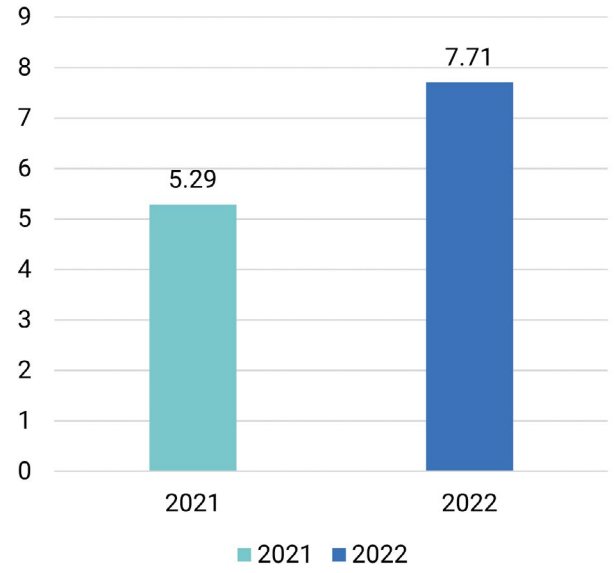


Q12. What impact, if any, do you think that the bot attacks have had on your customer satisfaction in 2021??

It's good to see this change, while it may be incremental. Businesses have increased their budget for bot management from last year, which accounts for their greater visibility of bot attacks. However, the marginal gains made so far suggests that less than 8% of the total security budget—the average businesses are spending—is not enough.



Q13. On average, each year, what % of your business is being lost to competitors due directly to the impact of bots?



Q14. Do you have a dedicated budget for bot management, if so what percentage of your overall security budget does it represent?

A better understanding?

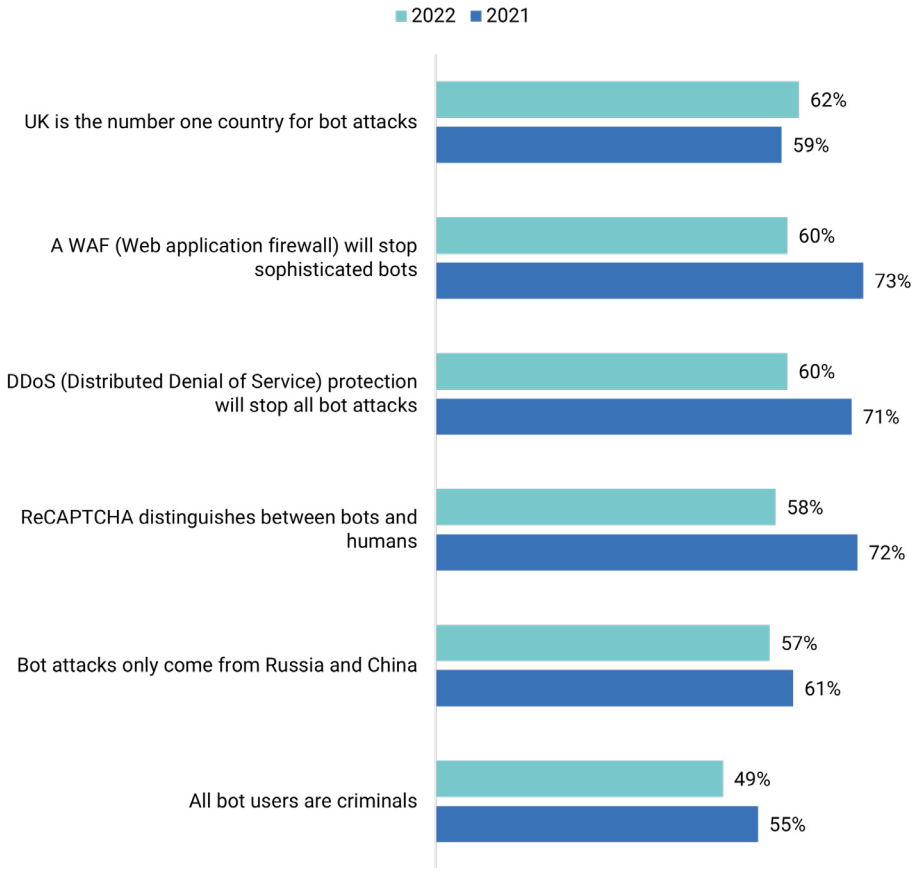
Undoubtably, there has been a marked improvement and increase in awareness and investment, but there are still huge misunderstandings around the origin, intention and complexity of bot attacks.

Since our last survey, more than 50% of respondents still believe bot attacks only originate from Russia and China. Whilst our research shows attacks have increased from both, businesses must not forget that attacks also originate from the UK, USA and Europe.

As bot attacks get smarter, so must mitigation strategies. Blanket bans on traffic based on the country of origin can leave organisations vulnerable from bots attacking via proxy and other common locations.

There is also still confusion amongst businesses when it comes to intention and legality. Forty-nine percent of respondents believe that all bot users are criminals–but this is not true. While credential stuffing and account takeover attacks are rightly illegal, it is not currently illegal to buy up high-demand items for resale.

Although there is a long way to go, more businesses are recognising that bot mitigation tools like reCAPTCHA are not a complete solution for increasingly sophisticated bot attacks. But far too many think that WAF and DDoS protection alone will help prevent them.



Q14. Are these statements about bots true?

Conclusion

The way businesses are catching on to bot attacks is reflected in their attitude to resellers. In 2021, only 29% of businesses thought that customers would pay a markup for in-demand goods. That number is now 57%.

We know for certain that customers will pay a markup, the media reports of successful scalpers shows just how willing they are. It's good that businesses are recognising this too, but 57% is way too low.

This sums up the trend in bot mitigation. There is progress in both understanding and tackling the problem, but this progress is limited. We are, at least, moving in the right direction—but we need to speed up.

The increase in attacks from other countries signals that bot attacks are not going to slow down any time soon, they will only shift in focus and origin, and sophistication. Despite increased investment from businesses to combat the problem, bot mitigation remains a small part of overall cybersecurity spending, limiting the effectiveness of any mitigation tools they put in place against increasingly sophisticated attacks.

As in 2021, the misinformation and misunderstanding concerning the origin, intention and complexity of bot attacks is prohibiting businesses from taking the appropriate action to mitigate the threat effectively. Most damning of all our findings is that businesses are taking longer to discover bot attacks than last year. While other metrics are improving, this important one is moving backwards.

Ultimately, businesses know that bots are a problem, and they also know which areas of their business are most vulnerable to attack. But where increased awareness and investment mark a step in the right direction, the sophistication and intensity of bot attacks threatens to push organisations back.

NETACEA

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.