NETACEA

The Bot Management Review:
Separating Bot Fact from Fiction

Contents

Introduction

Bots are damaging businesses, both directly and indirectly. Bot traffic costs businesses millions, whether they are scraping content, buying up goods before anyone else, or using stolen passwords to take over accounts.

Our research shows that bots cost businesses an average of 3.6% of their online revenue, but the problems run deeper. If businesses cannot tell the difference between real customers and bots, this can make marketing analytics data useless. Businesses have burned through marketing budgets and made poor decisions based on bad marketing data. Despite a lower profile, this is just as big a problem as ad fraud.

To fight an enemy, you must understand it. We wanted to know what businesses knew about bots—and what myths they still believed.
We interviewed 440 businesses based in the USA and UK, in eCommerce, telecommunications, entertainment (including online gaming and streaming), travel and financial services markets. Could they tell bot fact from bot fiction?

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

Enterprise organizations know that bots are a problem. Businesses are able to pinpoint where bots are affecting their revenue and understand that bad marketing decisions can be a result of data skewed by bot activity.

Unfortunately, that's where the good news ends. Many are confused as to what techniques and technologies are effective against bots, where these bots are being used, and who uses them.

Of most concern, is that over two thirds of businesses think that Web Application Firewalls (WAFs) and Distributed Denial of Service (DDoS) protection will keep them secure against bot attacks.

These tools are valuable and recommended but they are not effective against sophisticated bots—leaving businesses vulnerable to attacks that may be the difference between profit and loss.

Bots are being "democratised" and offered as a service, so the assumption that large nation states are behind all bot attacks, and are bought and sold on the dark web are completely out of date.

In the battle between businesses and bots, bots have the upper hand thanks to a lack of understanding. To beat bots, better knowledge of the enemy is needed—and that means busting these persistent myths!

The biggest myths

We asked businesses to decide whether a number of statements were true or false. Some of these were true, some false, some are mostly myth based on a little truth.

These are the myths that most businesses believed to be true.

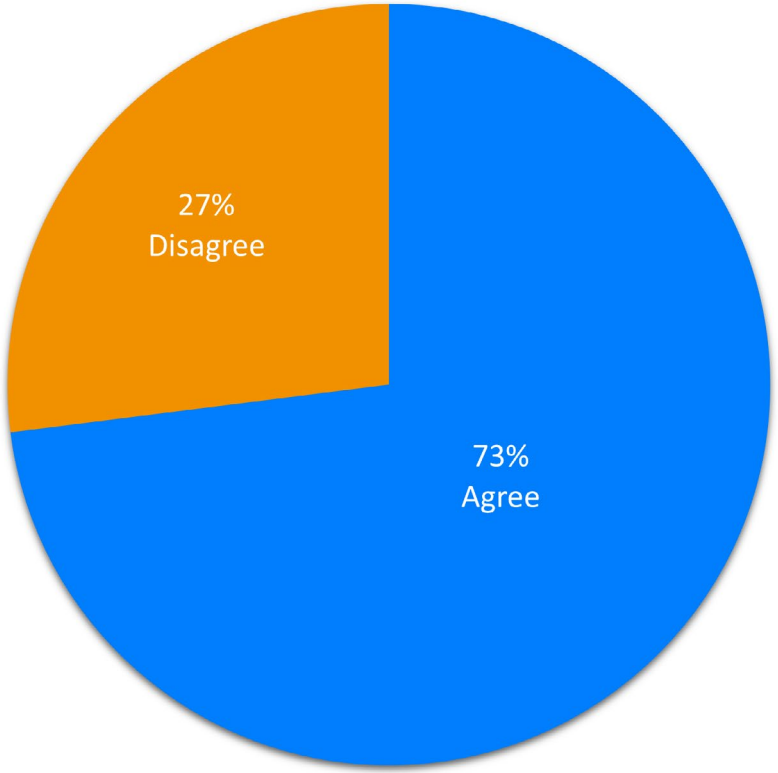
FALSE: A Web Application Firewall (WAF) will stop sophisticated bots

73% of respondents believed this myth—including 92% of telcos and 77% of eCommerce businesses.

WAFs are designed to prevent attacks that target vulnerabilities in security, through techniques such as injecting code. But many bots exploit websites by attacking "business logic"—no security holes are needed.

For example, a bot can hold an item in a basket for resale on another site, only checking out when the sale goes through. This is not exploiting any faults in the code, the attacker simply uses an understanding of how the site works against it. A WAF will not help here.

Many WAF providers also offer basic bot mitigation, and it's possible that this is where the myth comes from. In our experience, many of these "add-ons" are ill-equipped to cope with the increasing sophistication of bot attacks. It's important to understand that bots are looking to take advantage of a website, mobile app or API working as intended, rather than injecting code to change how it operates.



FALSE: Distributed Denial of Service (DDoS) protection will stop all bot attacks

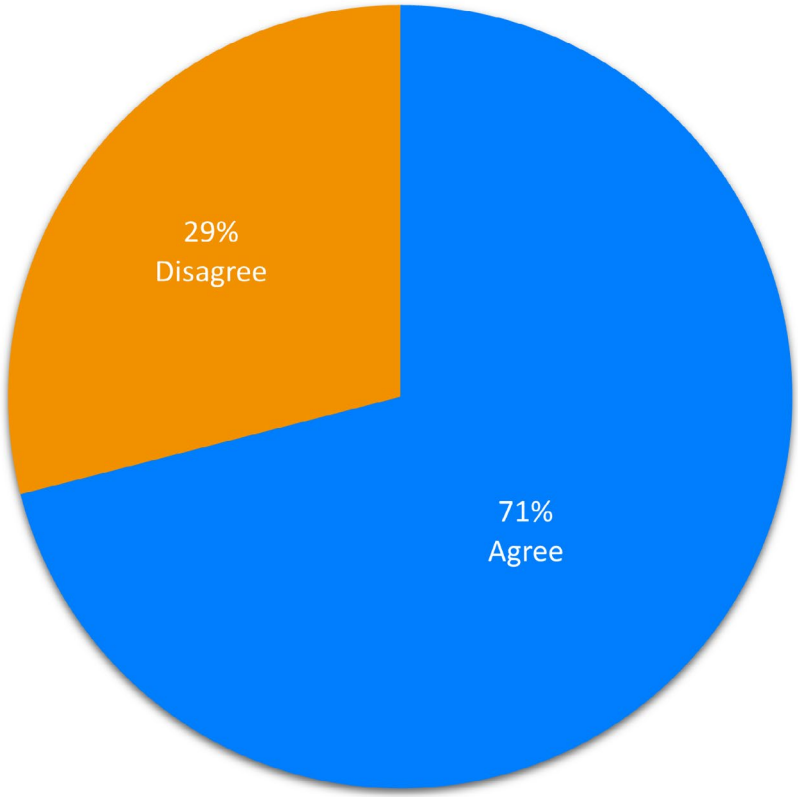
71% of respondents believed this myth, but there is no truth in it at all.

A DDoS attack will overwhelm a site with traffic, using a network of compromised machines, also known as a botnet.

Bot traffic is different. Unlike botnets, bots look to take advantage of sites, not take them offline. Taking a site offline means a bot attack will have failed.

While bots are capable of overwhelming a site with traffic, they will often limit how frequently they repeat actions to avoid “rate limiting” protection. More sophisticated bots can even learn rate limits for specific sites to better avoid them.

There is a great deal of confusion over what is meant by a bot, and the term “botnets” doesn’t help. We’ve also experienced confusion over bot attacks and social media bots designed to seed misinformation. Businesses must learn the difference between these automated attacks—and also the various types of bots they are at risk from, whether that is scalper bots, scraper bots, account checker bots, or any others. DDoS protection will not secure against such attacks.



FALSE: Bot attacks only come from Russia and China

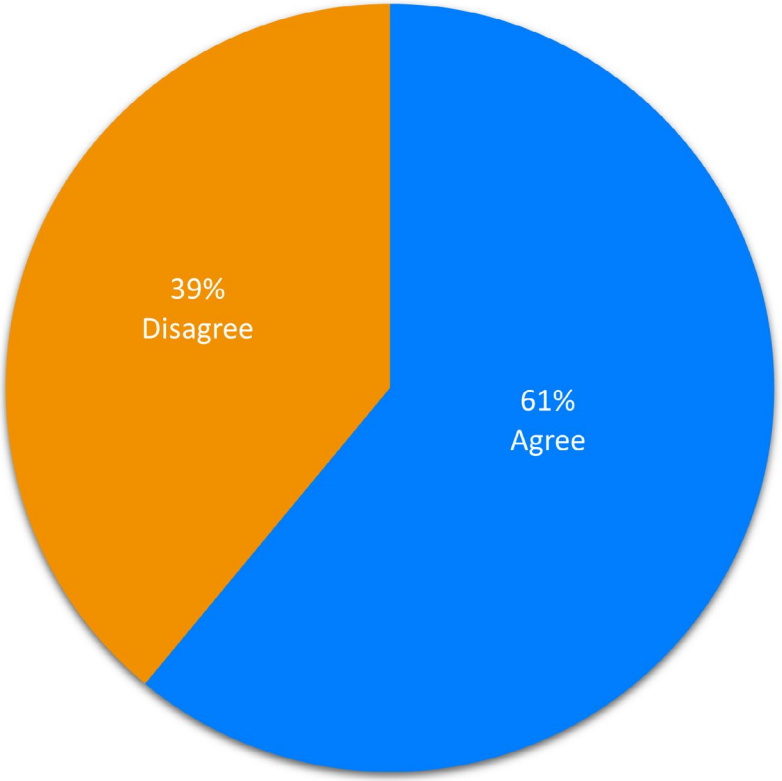
It's true that many bot attacks come from Russia and China, but it's also true that many originate from the UK, the USA, and all around the world.

Our research has found that just over a third of businesses have detected threats from Russia and China. Meanwhile, around half detected threats from the USA (51%) and the UK (46%), and many more (75%) detected threats from Europe.

In recent years, there have been many media reports into how Russia in particular may be using social media bots to influence elections and other events. But the bots that businesses should be most worried about are not run by nation states—they are operated by people out to make a profit. These can be professionally run businesses or amateurs, but they are just as likely to be in the same country as located abroad.

Beyond elections Russia has also been using bots to try and spread their government's version of events in Ukraine both within Russia and external to it. These bots have been harnessed as a tool of cyber-influence operations around the world.

Of course, we shouldn't completely ignore the threat from Russia and China, but as the threat doesn't always come from foreign actors, simply banning traffic based on the country of origin is not an effective bot mitigation strategy. We need to be smarter than that. Bot operators may also use proxies to impersonate legitimate users from another country, making restrictions based on country of origin even less effective.

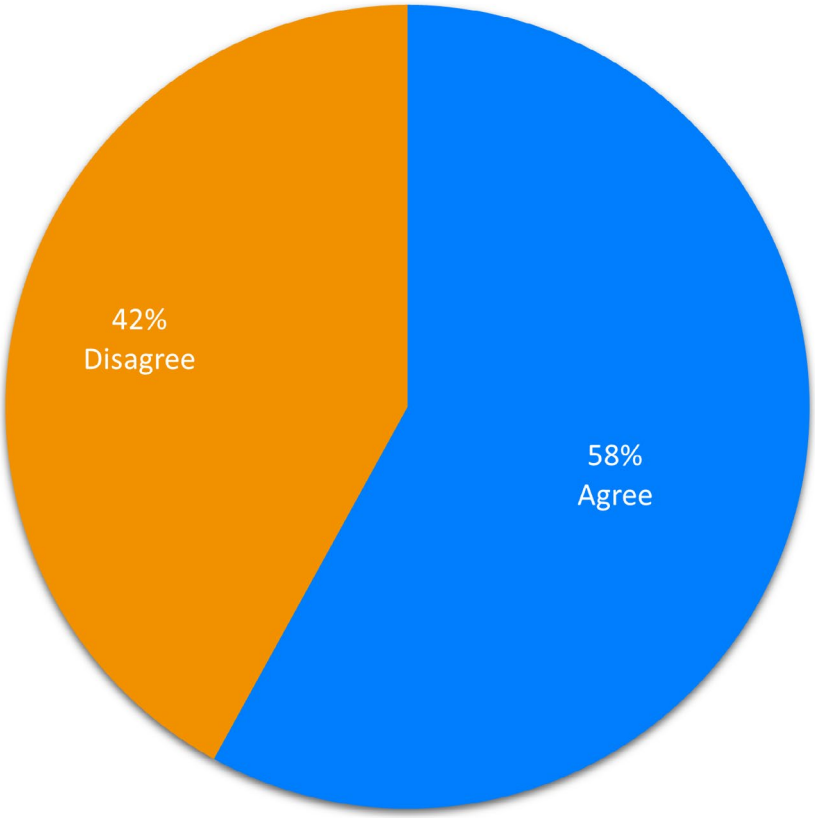


FALSE: You can only buy bots on the dark web

Increasingly we see not just bots, but “combo lists” of usernames and passwords available on the “clear web”, accessible to everyone. And as people are unable to buy goods, such as games consoles, using traditional means, they are turning to bots to beat the rush. And the bot market is responding. Interested buyers no longer have to navigate the dark web to get what they want.

Also common are “bots as a service” where hackers offer their services to those willing to pay. Increasingly, bots require zero technical knowledge—just the right website and a way to pay.

A few years ago, this idea that the dark web was the only route to buying a bot may have had some truth, but no longer. Many bot operators are now professional businesses, and to thrive they are making their services available to a much wider audience. What this means for businesses is that there are many more people looking to subvert their websites—trying to take over accounts, use scalper bots to buy and sell goods, and more. It also means the bot creators have an even bigger incentive to improve their bots and provide regular patches and updates—just like any other software-as-a-service provider.



Misleading factoids

A “factoid” is a piece of unreliable information that is repeated often enough that it becomes accepted as fact. Sometimes pieces of information are just unreliable or misleading enough to be problematic. Here we’ve collected a handful of “near-myths”—not quite false, but misleading if a business believes it without question.

NEAR-MYTH: ReCAPTCHA distinguishes between bots and humans

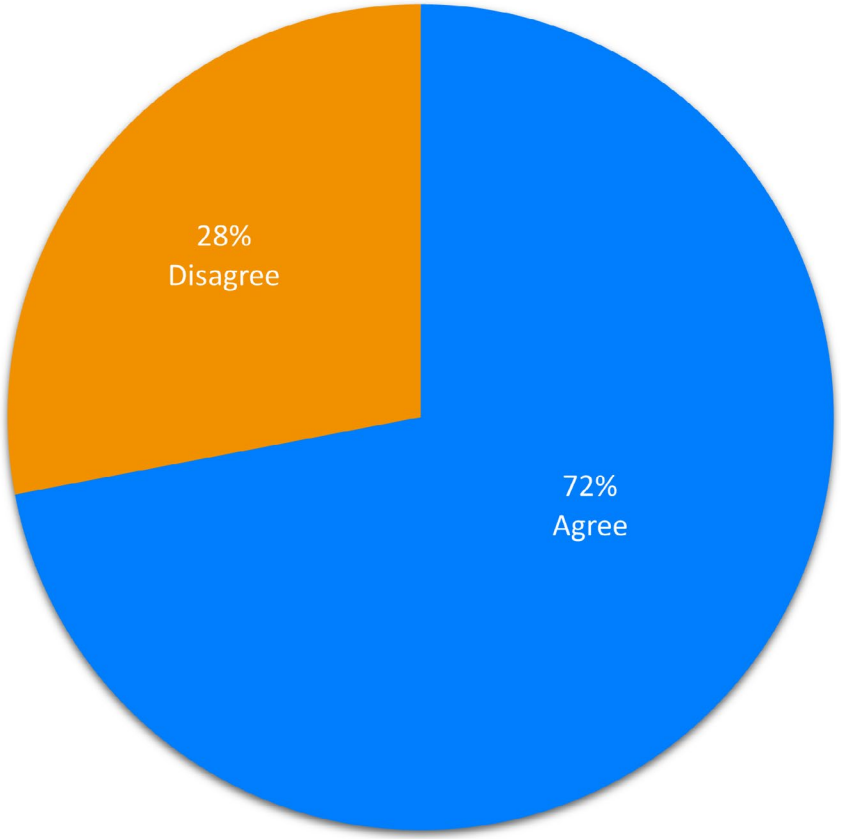
ReCAPTCHA and similar techniques do help to distinguish between bots and humans. But it is not 100% effective—more sophisticated bots will be able to circumvent this technology.

CAPTCHA techniques are in an arms race, trying to stay one step ahead of bot creators. They are an incredibly useful tool, but not a complete solution on their own.

CAPTCHA has a place in bot mitigation, but it cannot be the only solution in place. Customers don’t like to have to solve little puzzles when visiting a site, and if asked to they are much more likely to browse elsewhere.

As bots get better at solving these puzzles then the puzzles must become more difficult and more frustrating. Even if we were able to solve the problem and create uncrackable CAPTCHAs, it’s possible to outsource solving them to CAPTCHA farms, where puzzles are outsourced to low-paid workers to solve for pennies.

CAPTCHA is a bot mitigation technique, not a complete solution—it is a useful part of the toolkit, but can’t be relied on to deal with the problem alone.

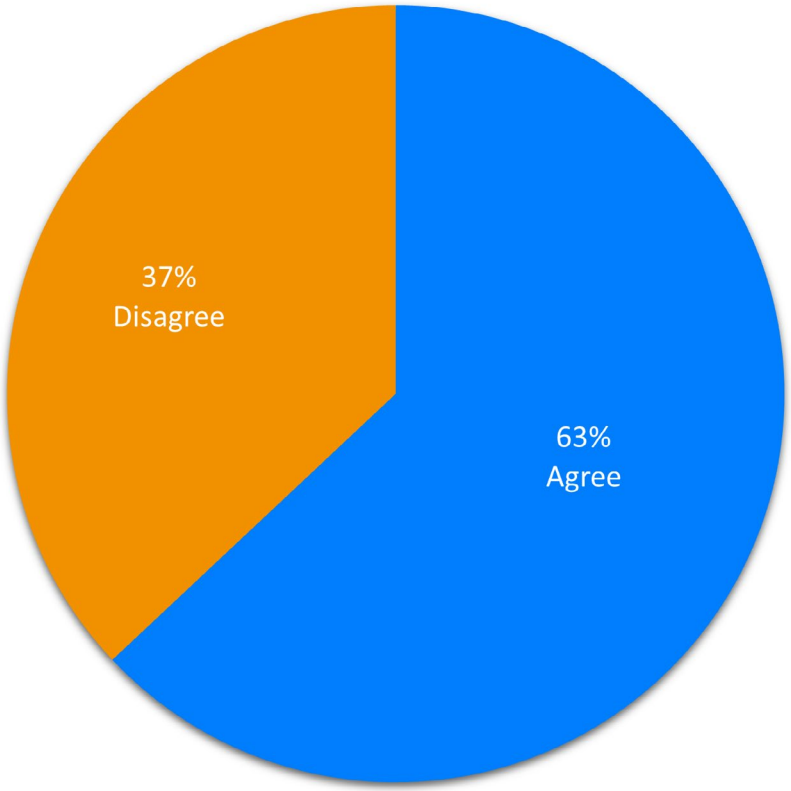


NEAR-MYTH? Most bot traffic comes from data centres

Hackers do often use data centres to host their software and launch attacks, but will go to lengths to disguise the origin of their attacks. Simply banning traffic from data centres is not enough to protect a business from bot attacks.

One way to get around this is the use of “residential proxy networks”. Attackers are increasingly using compromised computers and mobiles as proxies for their attacks—sometimes by compromising the device without the owner’s knowledge or consent, but other times the users actually opt in, by downloading and installing software such as free VPNs, to “rent” access through their device to others.

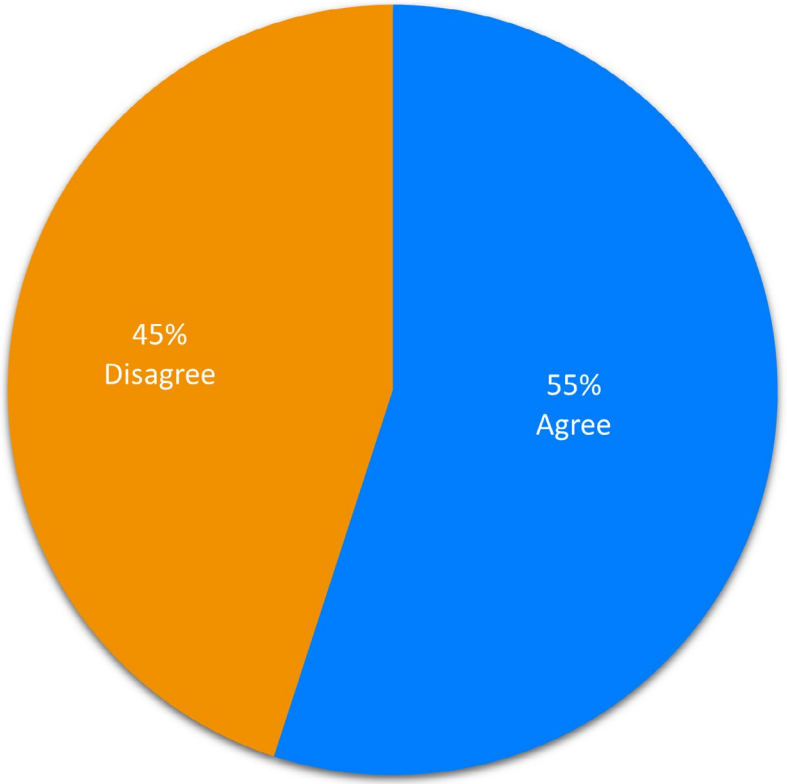
Knowing where traffic is coming from will help to identify attacks, but it is not foolproof. We can look at traffic from data centres and be pretty sure this is likely to be bot activity, but not all bots are bad! All sites rely on search crawlers for good SEO, and many retail sites rely on scrapers that report prices to comparison sites. Separating good and bad bots is just as important.



MYTH? All bot users are criminals believed by 55%

At the time of writing, there are plans for laws to ban “grinch bots” or scalper bots in both the USA and UK, but the laws are quite some distance from being enacted. So, while account takeover and card cracking attacks are clearly illegal, using a bot to buy up goods for resale is not yet a criminal act.

What is a criminal? Not everyone using a bot is doing so to break the law. There are some who undoubtedly are, like those who are trying to use stolen passwords to take over accounts, or those who are checking the validity of stolen credit cards. But there are those who are in more of a grey area. People are using bots more and more to buy goods that are in limited supply, and easier access to bots means this is more likely to be “normal people”, people who would never consider any other kind of nefarious activity.



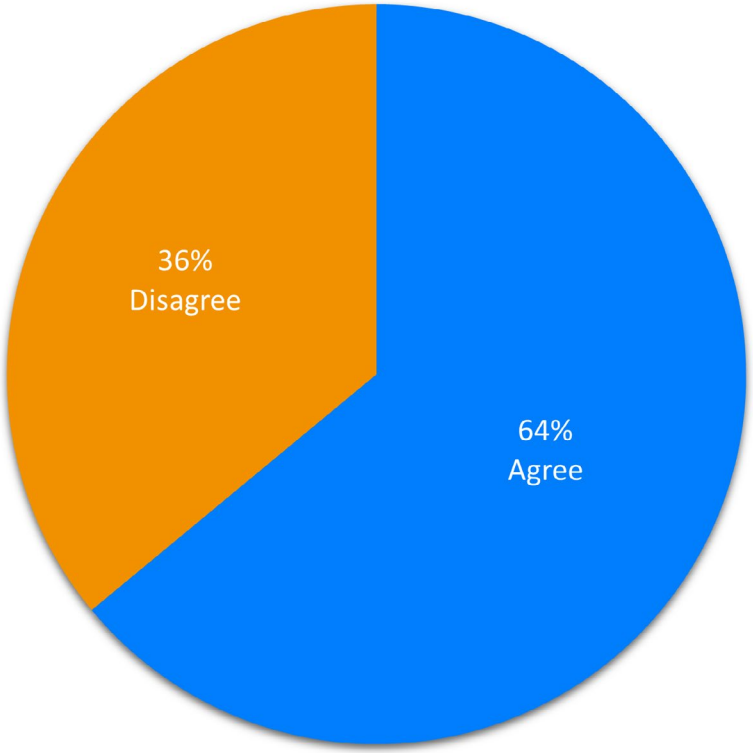
Facts about bots

Not every statement we asked about was false. Businesses were better at identifying the statements we presented that were true.

TRUE: The majority of credential stuffing attacks use bots or automated technology

Huge “combo lists” of stolen usernames and passwords are available for sale on the dark web. It’s impossible to check their validity manually, and so hackers will use bots to sift through these, checking for accounts they can steal and sell.

We can ask our customers not to reuse passwords, but unlike blocking simple passwords there’s no way to make sure they will be careful. So, when another unrelated service loses all of their passwords in a data breach, some will unlock accounts elsewhere. Bots automate this process and make it simple. Bot mitigation is not just about protecting your business, but also protecting your customers from their own bad security habits.

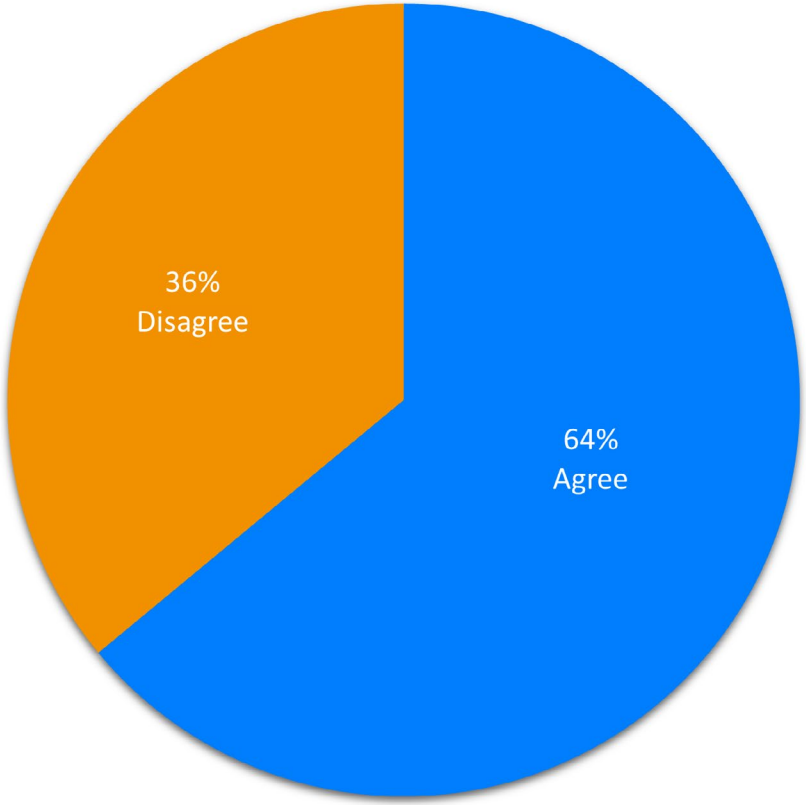


NETACEA

TRUE: Advanced persistent bots are becoming more common

Some hackers are opportunistic, and will attack sites for a short period, grab what they can, and leave. But it is increasingly common for more sophisticated bots to be far more targeted and try to leave no trace behind when stealing data.

Advanced persistent threats (APTs) of all types are appearing with greater frequency. Just as there are more amateur hackers taking advantage of available services, sophisticated hackers are moving towards being more targeted and tenacious. They will target a site relentlessly, looking for any crack in the armour to exploit. Businesses need to beware not just of more attacks, but more sophisticated and relentless attacks.



Conclusion

Our previous research found that enterprise organizations know that bots are a problem, and they recognise where bots are affecting their business. They know that bots affect their bottom line and that this is a problem that needs to be tackled.

However, there are persistent myths about bots that refuse to die. Enterprises are:

- Confusing bots and botnets and think DDoS protection will keep them secure against all bots.
- Unaware that bots are using their own business logic against them, and think that CAPTCHAs will solve the problem.
- Unsure about where bot attacks are coming from, believing that the biggest threats come from China and Russia when the real problem is more likely to be next door.

Businesses cannot manage the threat of bots without a better understanding of what they are and what they are trying to achieve. As the less well-known Sun Tzu's quotation says, "If you know yourself but not the enemy, for every victory gained you will also suffer a defeat." Organizations that do not know how bots are being used against them will not be able to prevent these attacks.

An average of 8% of revenue is being wasted by a combination of serving bots and by poor decisions due to skewed analytics. Education is a must to tackle this.

What are bots costing your business? Head to Netacea's bot calculator to find out today.