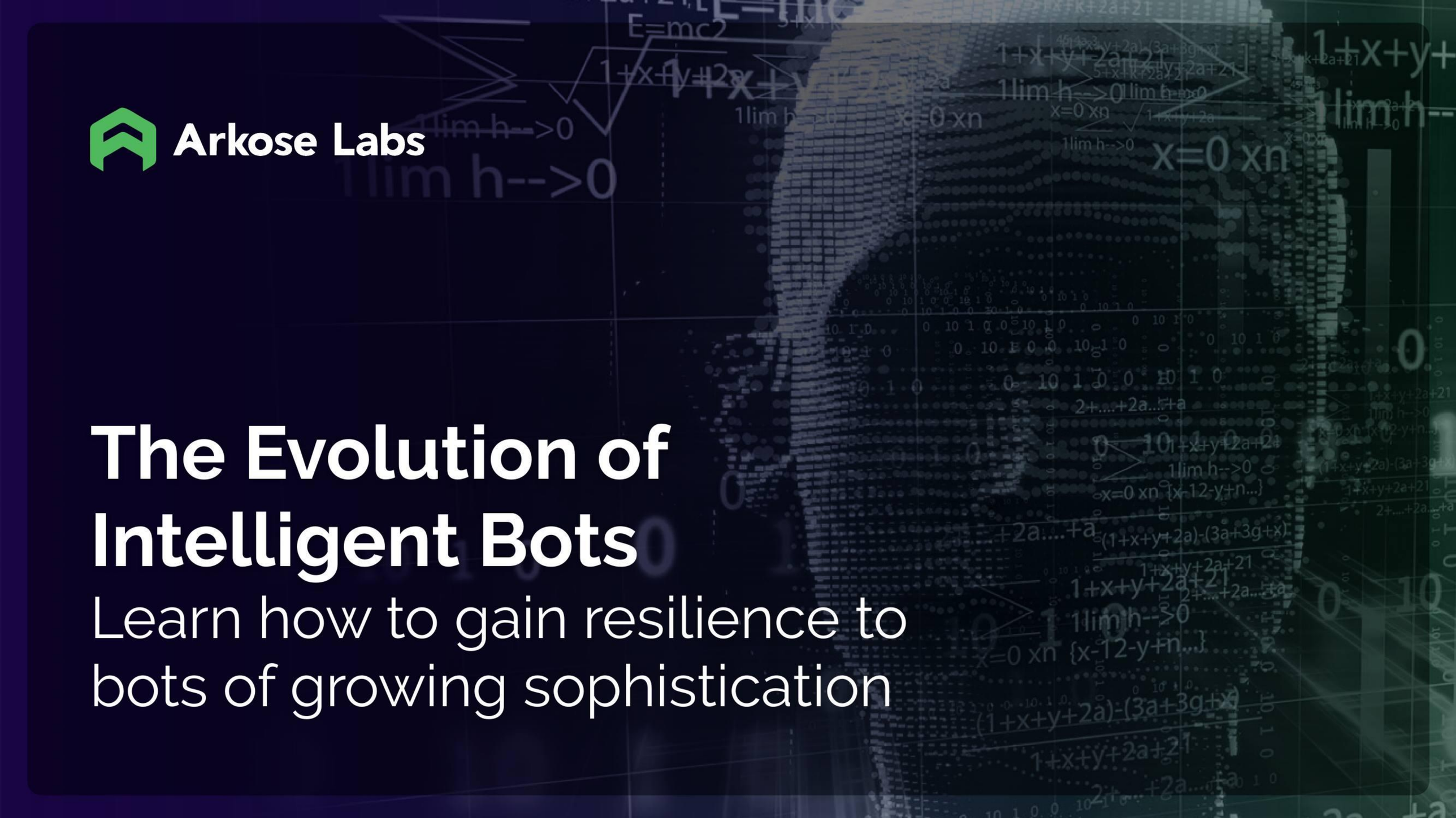


Arkose Labs

The Evolution of Intelligent Bots

Learn how to gain resilience to bots of growing sophistication

The Rise Of Intelligent Bots

Today's intelligent bots are becoming more nuanced and advanced by the day, able to bypass defenses and mimic good users with shocking accuracy, and power a complex orchestration of attacks, combining data, attack tools, and spoofing to emulate human behavior better than ever before. According to Arkose Labs data, the intelligent bots now have three times more signatures for fraud and more security teams to analyze than the previous ones, making accurate risk detection that much more difficult.

These bots are indispensable in carrying out fraud and cybercrime. In fact, automated attacks compromised 86% of the number for 2021. They allow attackers to launch thousands of attacks in a matter of seconds and achieve far greater profit.

Digital businesses need to be more innovative and agile to keep up with the volatile and complex bots of the future. Businesses' internal fraud and security teams have to collect and analyze extensive data points in order to track, detect, and stop these bots as soon as they appear. As bot attacks get more sophisticated, so too must the defenses used to stop them.

In this ebook, we'll discuss the nature of the intelligent bot revolution, why these bots differ from automated scripts used for attacks in the past, and why they're more difficult to detect. Businesses will learn the most effective ways for detecting and stopping these intelligent bots, and how they can ensure their customers and platforms are protected from advanced attacks, leading to cost savings and a better return on investment.

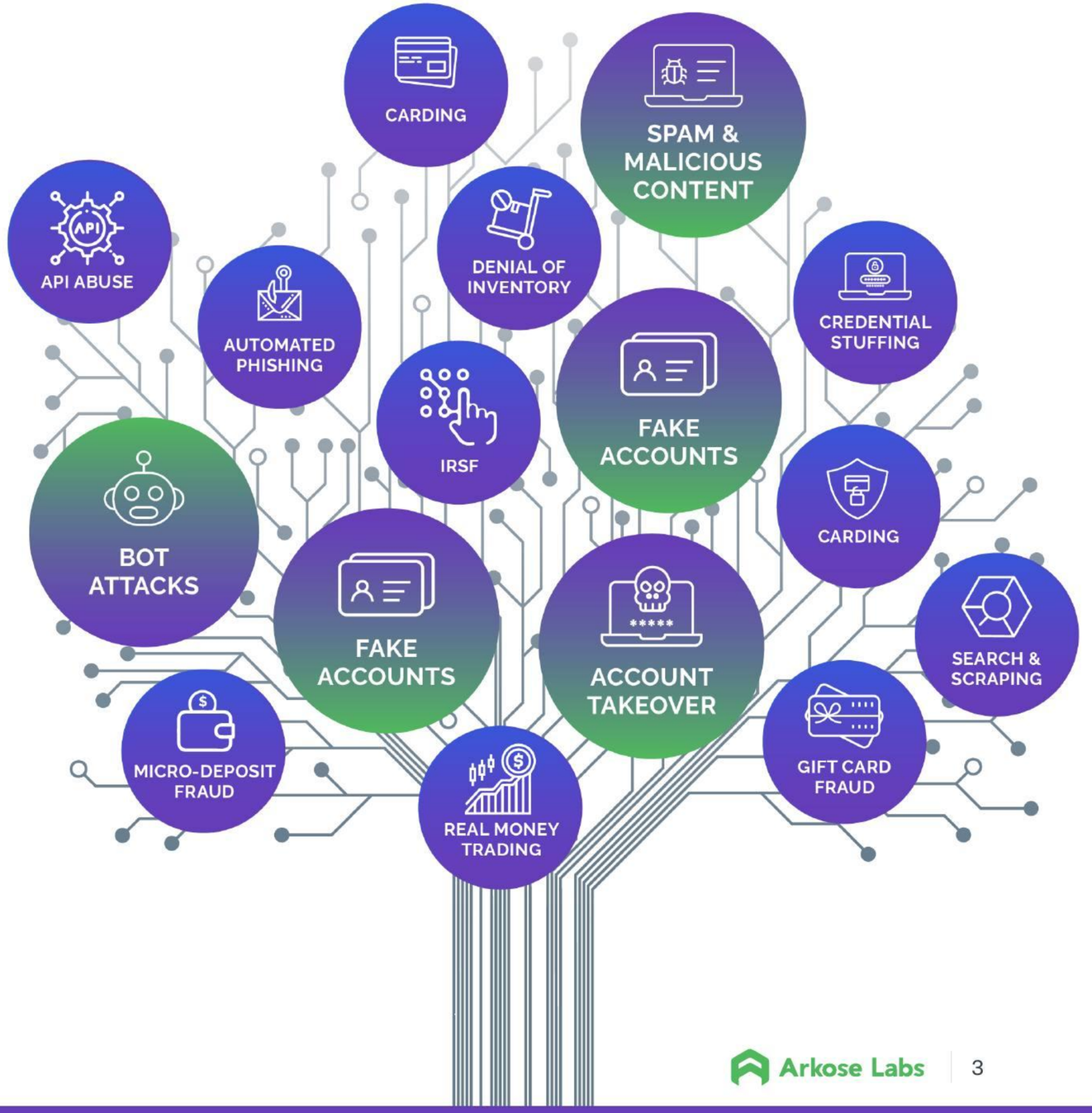
The Many Varieties Of Bot Attacks

Bot attacks are not one-size-fits-all. Different bots are used for different types of attacks, which have different routes to monetization. Some of the most common bot-powered attacks include:

- *Digital perimeter* - Attacks that target the digital perimeter often focus on stealing data or impacting the usability of a platform. This can include content scraping, either for competitive purposes or to resell the information, as well as inventory hoarding.

- *Account security* - Bots are frequently used to compromise account security. For example, they can be used to do credential stuffing to take over real user accounts or can then be used for bonus abuse to create fake new accounts. These fake accounts can be used for bonus abuse, fake reviews, or spamming and abusing good users.

- *In-app attacks* - Intelligent bots are also used to conduct a variety of malicious actions inside of applications as well. This could involve creating fake listings, cheating at games, or manipulating in-game environments.

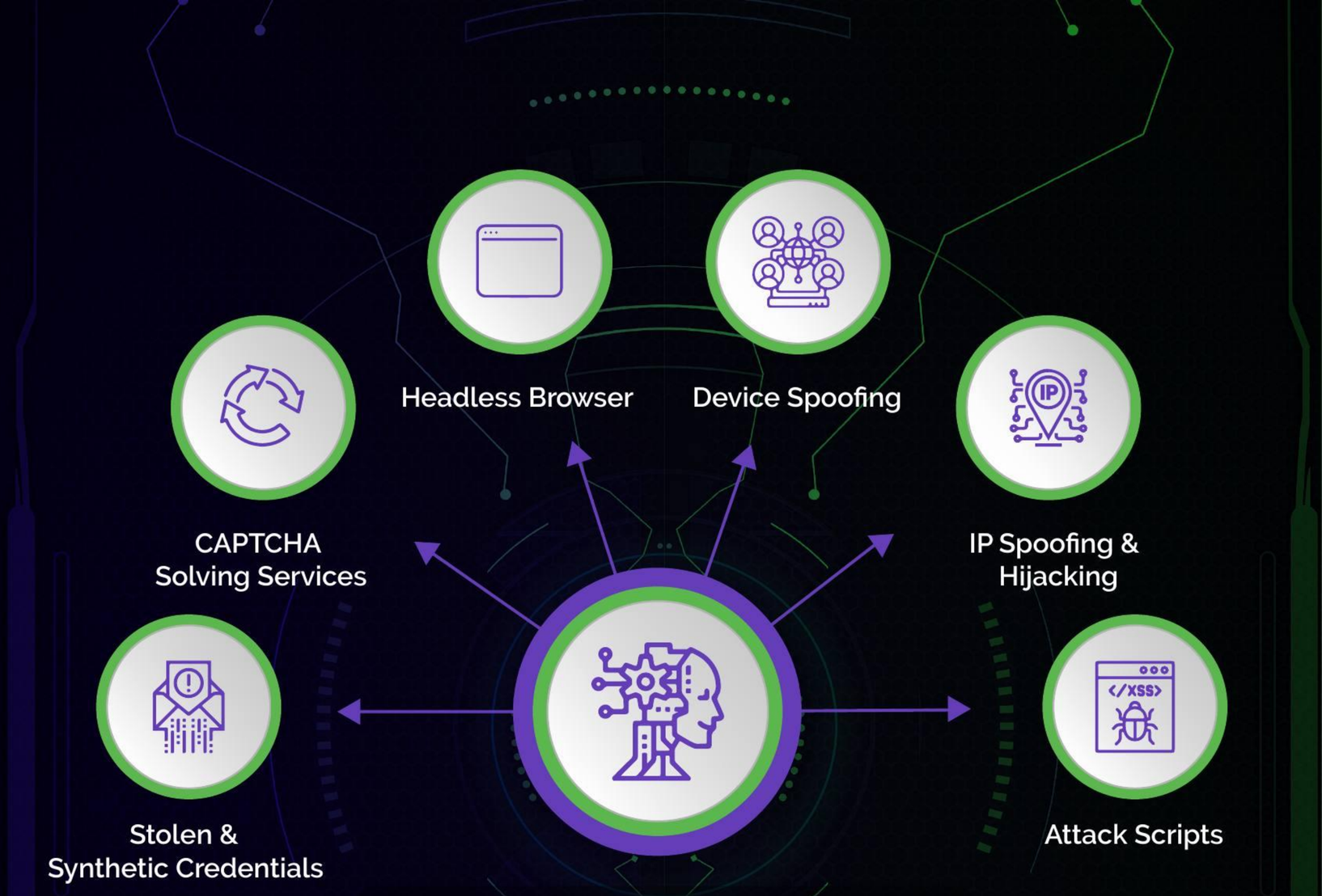


What Is An Intelligent Bot?

Bot attacks are growing in sophistication as well as data complexity.

They are increasingly accurate at spoofing and emulating human behavior, meaning more manual reviews for internal teams. This, in turn, leads to operational inefficiencies and increased costs.

Intelligent bot attacks also enable a number of routes to monetization for the fraudster, including stealing and reselling information, inventory hoarding, bonus abuse, and much more. By preventing cyberattacks, businesses can save money and increase their return on investment (ROI) by reducing losses associated with stolen information and inventory, preventing bonus abuse, and minimizing other damages caused by malicious attacks.



3x more complexity in detecting bots as they deploy a range of attack techniques

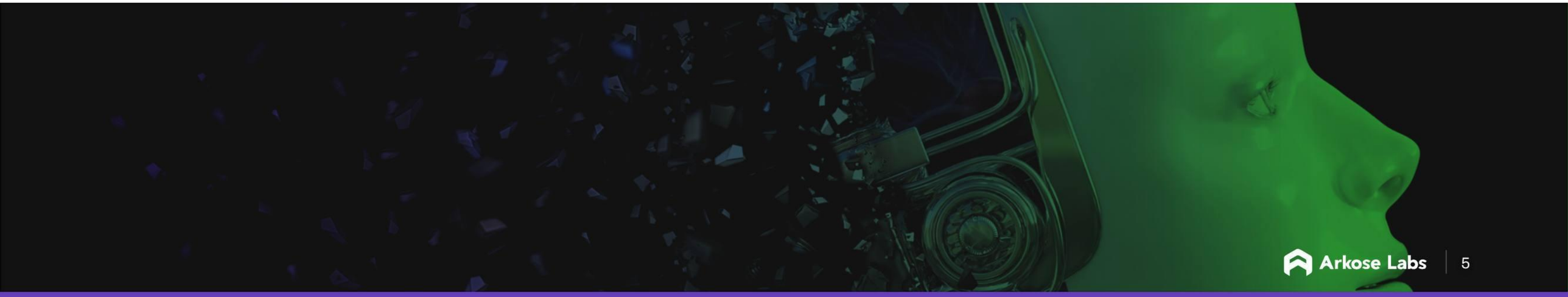
Bots Are Evading Traditional Defenses: Here's How

Many businesses today realize that detecting bots is not as straightforward as it used to be, because intelligent bots can bypass traditional defenses that attackers have studied and learned to work around.

- Bots can be made to appear as if they are humans when interacting with a website or login form. Reactive fraud solutions that rely only on known patterns and historical data are fairly ineffective because fraudsters use Artificial Intelligence (AI) to evade detection and present signals meant to deceive most bot detection systems.

- In the past, it was fairly easy to tell a bot from a human, based on factors such as IP address and device information. Now, attackers use methods like IP obfuscating, headless browsers, and keystroke and mouse movement tactics to make bots appear human.

- AI-powered bots are often "taught" in areas such as natural-language understanding and computer vision technology, meaning they are smarter and harder to detect than ever before. They can mimic human interaction with a website with a stunning degree of accuracy.

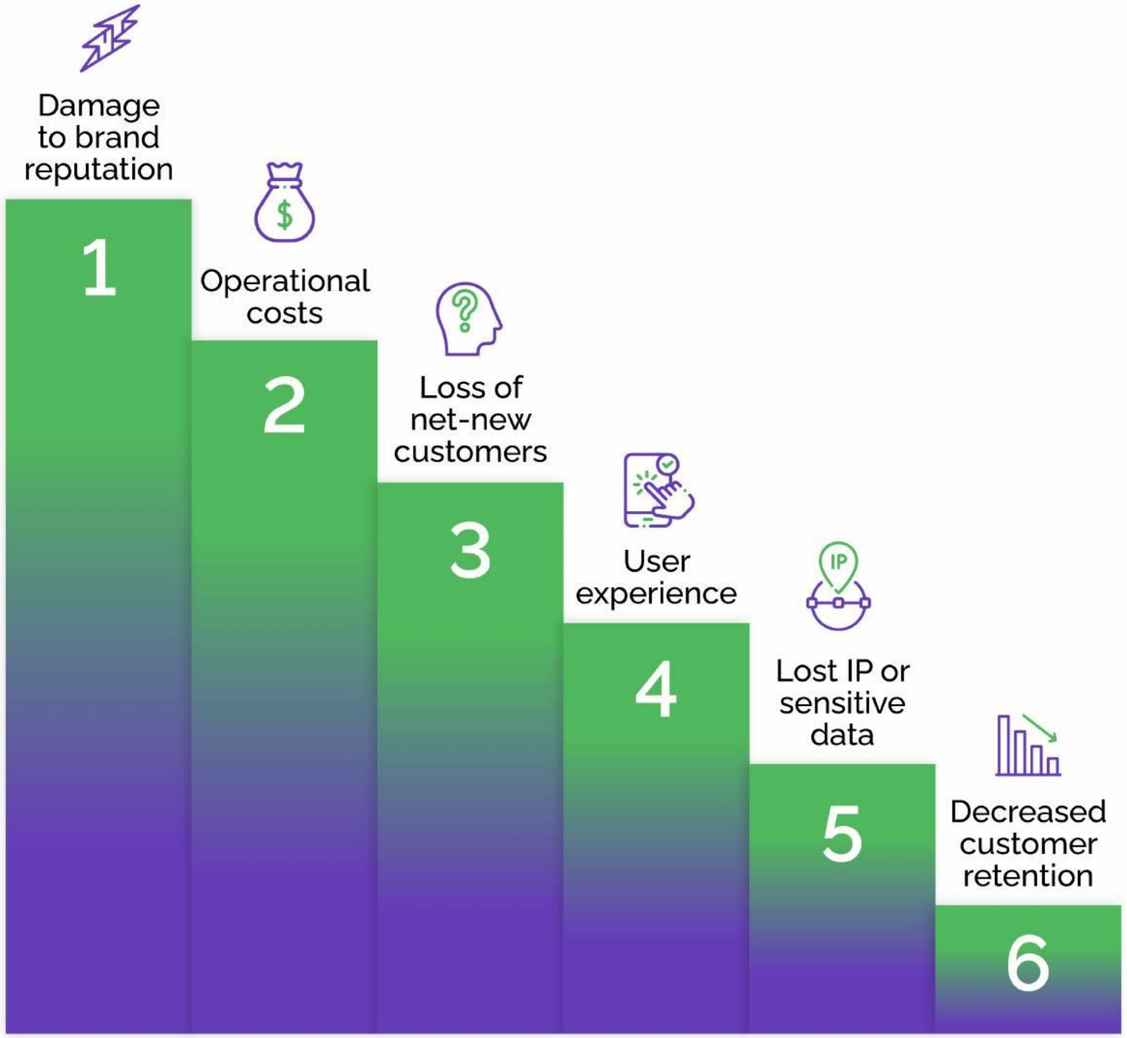


Bot Attacks Affect Consumers' Perception Of Brands

Bot attacks can have a major impact on businesses with a large or growing digital presence. To find out how bot attacks affect business, Arkose Labs conducted a survey of IT leaders in conjunction with market research firm Pulse.

One major takeaway from the survey was how these attacks can affect brand reputation in a number of ways. For example, if customers' accounts are being hacked, or they are continually targeted by spam and phishing attacks, they will take to social media to voice their complaints.

Furthermore, if the company falls victim to a large enough attack, it will likely generate news headlines and negative public relations. This will cause damage to brand reputation that could take months or years to recover from. Investing in cybersecurity measures to prevent cyberattacks is a wise business decision that can result in significant cost savings and a better ROI. Not only does it reduce the risk of a damaging attack, but it can also help to reduce the amount of time and resources needed to respond to and recover from a security breach. Additionally, it can help protect brand reputation, as the company will avoid any negative news headlines and public relations fallout from an attack.



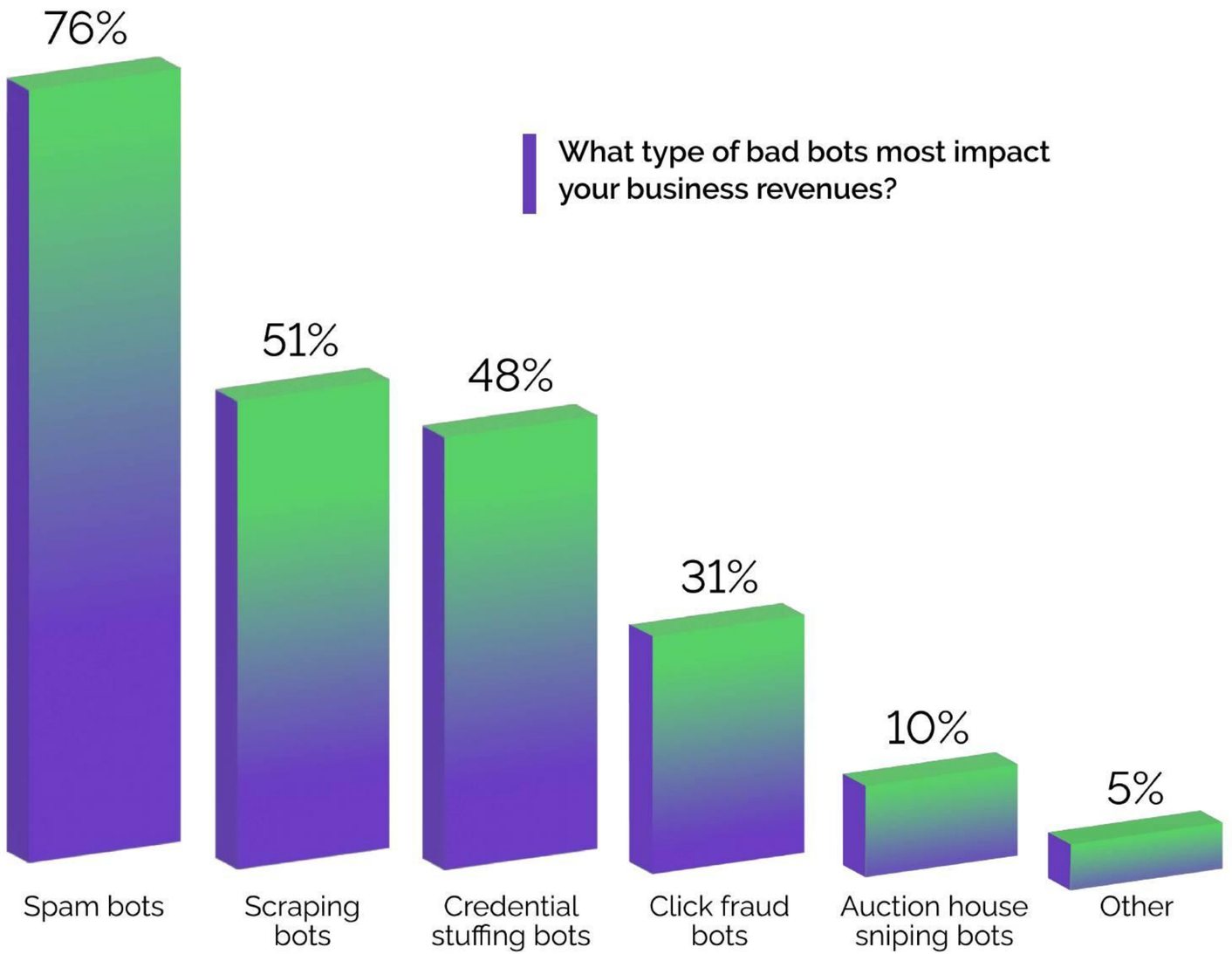
Source: Arkose Labs poll of 100 IT executives

The Financial Impact Of Bot Attacks

Bot attacks have a direct correlation on both business losses and lost revenue and failing to stop them can have a significant financial impact.

Businesses face financial losses due to account takeover attacks, including repaying customers for stolen money or items, resetting compromised passwords, and increases in contact center costs to address customers' security issues. Furthermore, when bots are scooping up in-demand inventory, businesses miss out on potential sales as consumers are driven to other websites. This leads to decreased revenue and cost savings.

As you can see in the graph on the right, our survey respondents identified spam bots as having the highest impact on revenue. This was followed by scraping and credential stuffing bots, which can affect customer retention, harm revenue, and diminish your ROI.

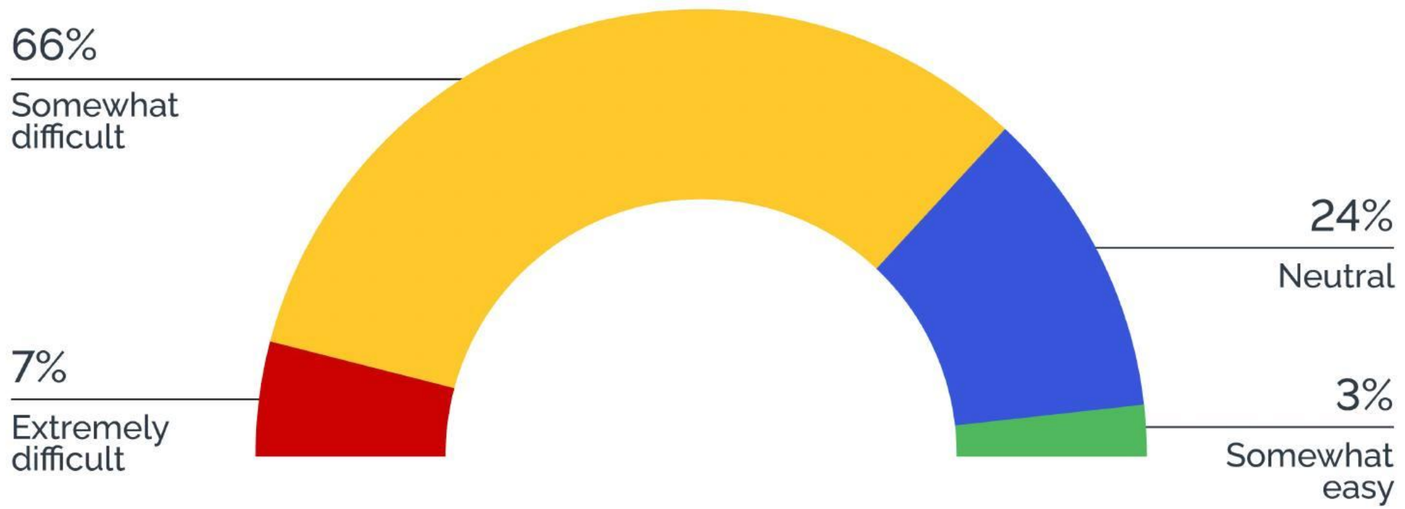


Bots Are Increasingly Hard To Detect In Real Time

The intelligent bot revolution has led to automated attacks that are extremely difficult to detect as they're happening. In fact, often it can take days or even weeks after the fact to detect an attack.

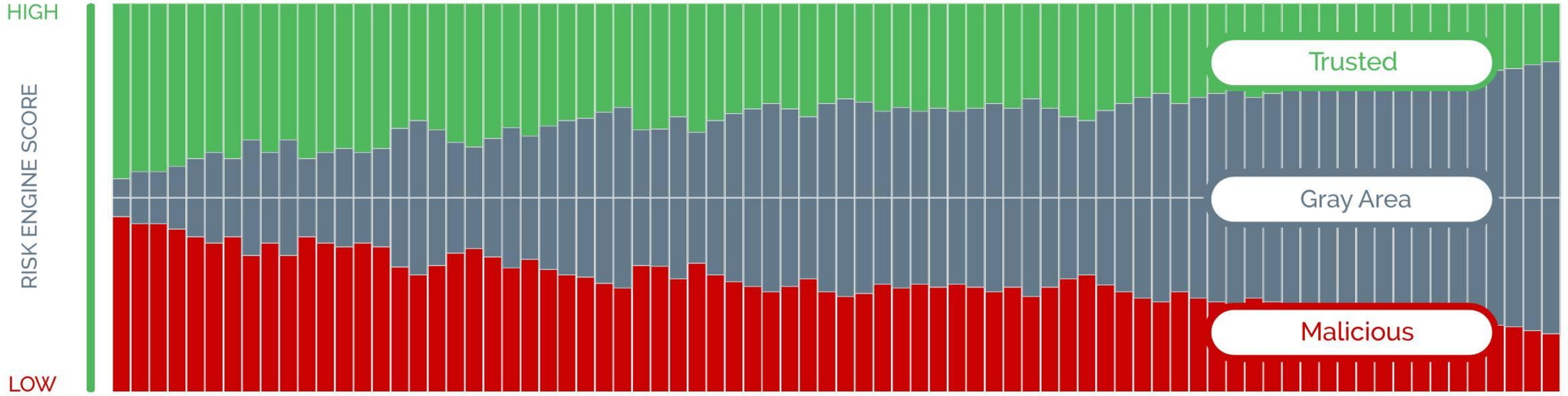
Nearly three-quarters of respondents said that detecting bot attacks in real time was either extremely or somewhat difficult. This is due to the complexity of intelligent bot attacks and how they can easily appear to be legitimate human traffic. This ability to "blend in" makes them difficult to detect as attacks happen.

How difficult is it to gain real-time insight into bot attacks as they happen?



The Difficulty Of The Growing Gray Area

Risk-based detection systems are dealing with a growing "gray area" of digital traffic, where risk signals often appear inconclusive. No matter what platform you use, this gray area is expanding as bots get smarter and stolen data gets richer. The growing gray area leads to user pain from false positives when good traffic is blocked as malicious, or false negatives when bad actors are allowed to get through. This creates difficulty for businesses, which could decide to block traffic showing inconclusive signals, but then run the risk of blocking good users. On the other end of the spectrum, being lenient allows too many bad bots through your defenses.



Why Is Detecting Intelligent Bots So Hard?

Dealing with potentially bad traffic is a difficult line for businesses to toe. They may not want to block traffic outright for fear of hindering good users. Instead, many organizations deploy some manner of challenge-response mechanism that is designed to stop automation, but is easy for good users to solve and self-remediate. However, many of these challenges fail on both fronts. Advances in machine vision technology mean most bots can easily solve them, while good users become frustrated.

Limitations of current approaches

Binary Block/Accept

Traditional methods are not transparent in showing how they assess risks, leading to a black-box situation which customers have to blindly trust.

No Feedback Loop

There is no way for customers to provide feedback on user activities, risk scores and response actions to train the models to make better decisions.

No Data Access

Customers do not have access to the risk data collected from their own environments, to use in their own models and help with downstream decisions.

No Customer Support

Customers are reliant on online forums or articles but there is no dedicated managed service team to provide hands on support when required.

The Risk Of Banning Good Users (And Good Bots)

Many of the bot prevention solutions used today have difficulty telling humans apart from automation, presenting a number of problems beyond successful automated attacks getting through. Not only do these false positives lead to a loss of revenue and customer churn, but also cause a significant amount of user frustration. This can lead to higher costs for customer service, as well as expensive customer retention efforts. Bottom line, the cost savings from an effective bot prevention solution can be substantial.

Good Bots

Search Engine Crawlers

Partner

Site Monitoring

Copyright

Aggregators

Bad Bots

Scraper

Spam

Click

Fake Googlebots

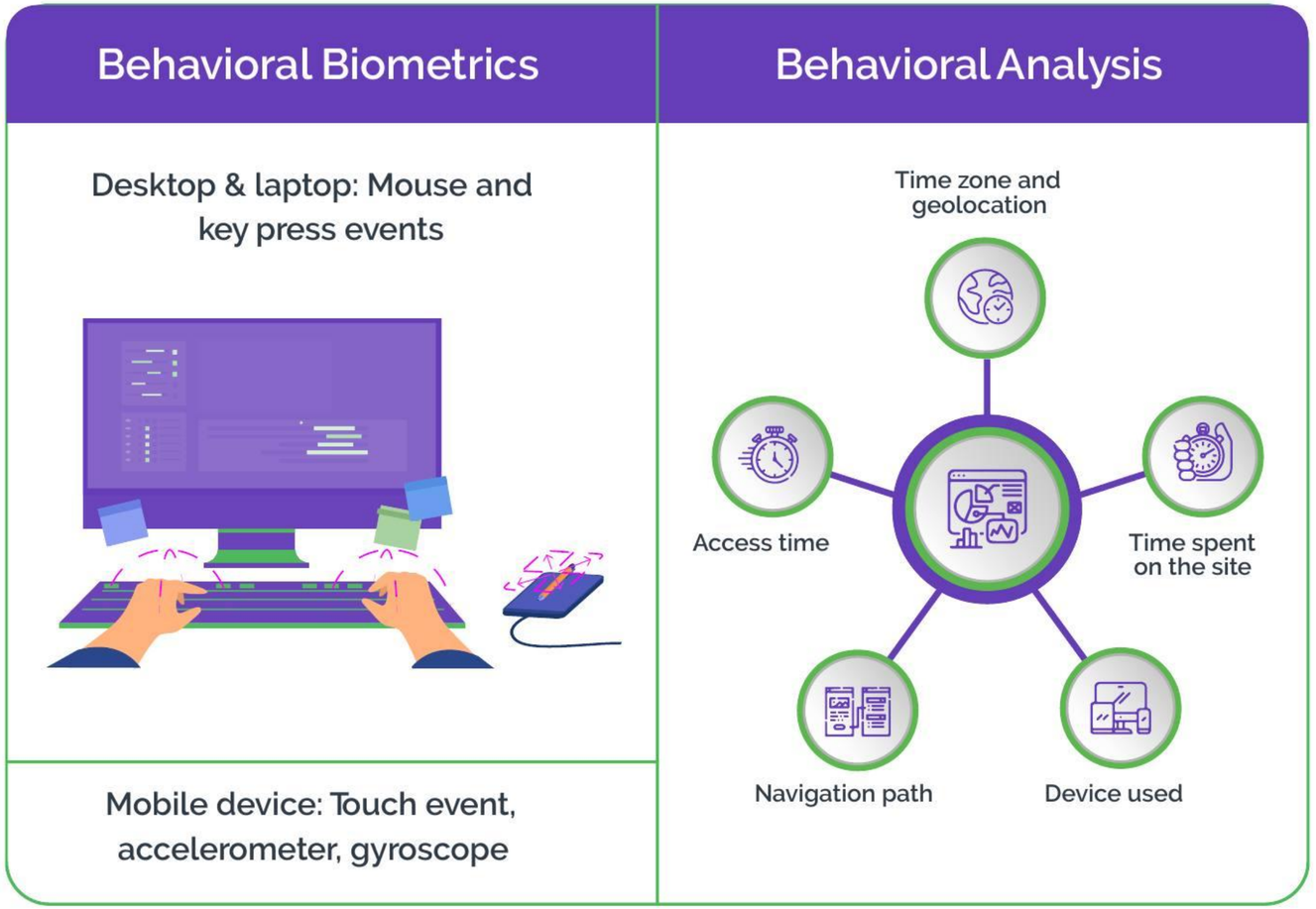
Botnet

The Role Of Biometrics And Analysis

Robust analysis of user behavior using both behavioral biometrics and behavioral analysis is also effective in detecting intelligent bots.

While behavioral biometrics examine the way a user interacts with a device, such as mouse motions, keystroke dynamics, or touch screen interactions, behavioral analysis looks at what a user interacts with in a web service and gives context to the actions they take.

Collecting this data can help identify attacks in a way that is independent of IP or device information, leading to a stronger detection signal. This not only helps differentiate humans from machines, but also results in significant cost savings by streamlining the security process. When these datasets are



How Businesses Can Respond

Though malicious bots are more sophisticated and harder to detect than ever before, they are not unbeatable. Here are some practical steps businesses can take to make sure they are properly armed and ready to face this intelligent bot revolution.

Find betters ways to manage inconclusive signals

- Bots should be detected and stopped, before they enter your ecosystem and wreak havoc. Utilizing a combination of rate limiting, IP and device intelligence, traffic shaping, and behavioral biometrics ensures attacks never go unnoticed
- Detection should also be user friendly so it doesn't impact good user throughput

Ability to deal with inconclusive signals

- Intelligent bots are able to mimic human users, which leads to the large "gray area" of inconclusive signals. This traffic should be challenged in a way that bad bots cannot pass, but real users can easily solve
- It's also important to utilize network data to detect new patterns quickly. Taking a consortium approach in threat intelligence by sharing data with other organizations helps to identify and stop evolving attacks

Sophisticated attack-response

- Businesses need to have the right defenses in place for specific bot types. This means taking a risk-based, graduated approach to pressuring suspicious traffic. This ranges from silent Javascript challenges, in-session user challenges, and shadow banning to, in the most extreme case, blocking (in the case of clearly malicious traffic)
- Companies should also employ tactics such as random traffic audits using a challenge-response mechanism in order to train and refine the detection engine

Checklist: Features Of A Robust Anti-Bot Solution

Here are some of the top considerations to keep in mind when looking for a bot defense solution:

Resilience to Advanced Attacks	User Experience	Vendor Partnership
✓ Robust AI-based Detection Engine	✓ Enables Smooth End-User Experience	✓ Ease of Set Up and Implementation
✓ Machine Learning Usage and Training	✓ Configuration to Allow Good Bots	✓ Out of the Box and Custom Reports
✓ Custom Threat Research and Intel	✓ Easy Good-User Remediation	✓ Provides Security Feedback Loops
✓ Explainability and Transparency in Decisions	✓ Complies with Data Privacy Laws	✓ Insight into Product Roadmap and Vision

The Arkose Labs Approach

At Arkose Labs, we have a unique approach to stopping the intelligent bot revolution.

Our AI-powered platform combines sophisticated attack detection, risk analysis, and the most innovative challenge-responses to defeat persistent bot attacks and coordinated human-driven attacks on the most targeted user action points.

A crucial advantage that our technology has is the continuous feedback loop between real-time bot detection, user challenges, and advanced analytics.

We use a wide range of different technologies to ensure that:

- We stop and deter attacks
- We provide transparency and support
- We provide excellent end-user experience
- We save the business considerable money in the long-run and deliver a more robust ROI

Conclusion: Stopping The Intelligent Bot Revolution

Sophisticated bots are proving to be increasingly harmful to businesses. They destroy brand reputation, hurt customer acquisition and retention, and drain revenue. Getting a handle on this pressing concern must be a top priority for all businesses that operate digitally.

Investing in the right tools and technology to stop intelligent bots is an essential investment for businesses. Utilizing IP intelligence and implementing sophisticated divide fingerprinting capabilities is an effective way to protect against malicious bots. A detection engine that uses probabilistic, statistical, and machine learning-based models can provide an additional layer of security. Not only does this provide a more secure network, but it can also lead to cost savings in the long run, not to mention a better ROI, as businesses can avoid the costly penalties associated with bots' malicious activities.

This type of security investment is important not only for business purposes, but also for creating a safer digital environment where all users know their data is secure and their accounts are protected from attacks.

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers the world's first $1 million credential stuffing warranty. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. Headquartered in San Francisco, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, Tokyo, and London, UK, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast500 ranking.

Offices

San Francisco
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

United Kingdom
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Schedule Demo