Report

Death by a Billion Bots:

The Accumulating Business Cost of Malicious Automation

NETACEA

Contents

Foreword

Andy Still

Co-Founder, Netacea

Automated customer interactions have underpinned digital business for as long as the Internet has existed.

An endless mass of checkouts, logins, inventory searches, gift card redemptions and more serve 5bn people globally, forming the critical infrastructure upon which a multi-trillion-dollar industry is built.

However, there's a darker side to this coin as threat actors have also noticed the value coursing through these interfaces.

Using bots they quietly target the APIs, websites and applications powering these automations to corrupt business logic at massive scale.

By doing so, they bleed revenues and abuse sensitive data wholesale, damaging reputation, degrading website performance and driving up technical costs.

Much like the early days of ransomware, a seemingly innocuous risk with consumer impact is quietly crossing the divide into the enterprise. Unlike ransomware though, its impact on corporate value is corrosive, rather than explosive, but no less harmful.

This is the problem we care about fixing and why we have done this research. One of the largest analyses of its type, we try to quantify the scale of the issue to help businesses understand just how much value is being lost to malicious automation.

Research overview

Summary findings

- Attacked companies state that the majority of malicious automation originates from Russia or China.
- The annual cost of bots is $85.6m per company – per year - dwarfing the average ransomware payment of $1.5m[1], and the equivalent of the eighth largest GDPR fine ever issued.
- Despite this, and in stark contrast to two-week[2] dwell times for threats breaching the internal perimeter, it still takes an average of four months for malicious automated attacks to be detected.

10
executive stakeholders

440
enterprises

$1.9bn
average online revenue

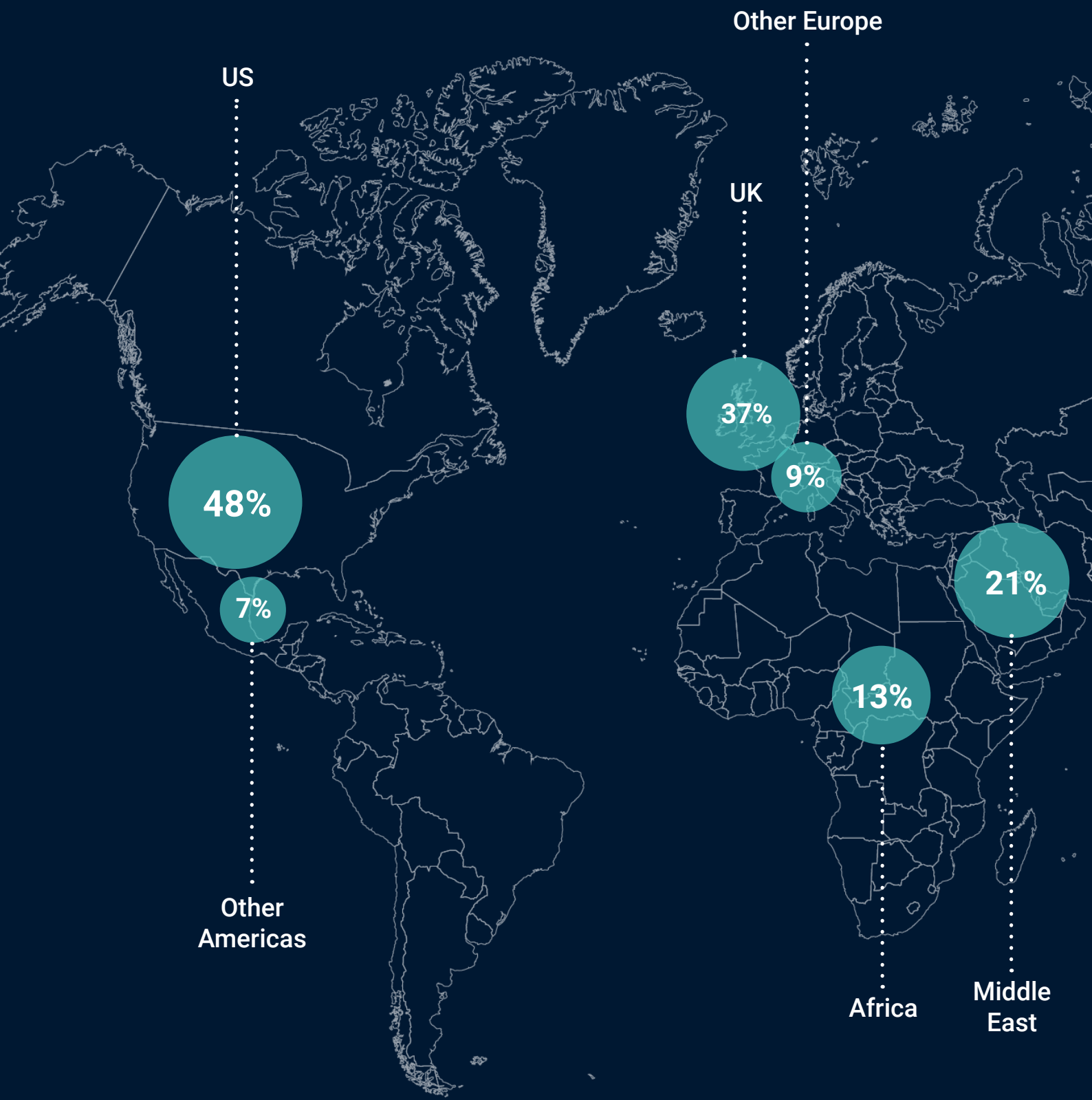
5
sectors

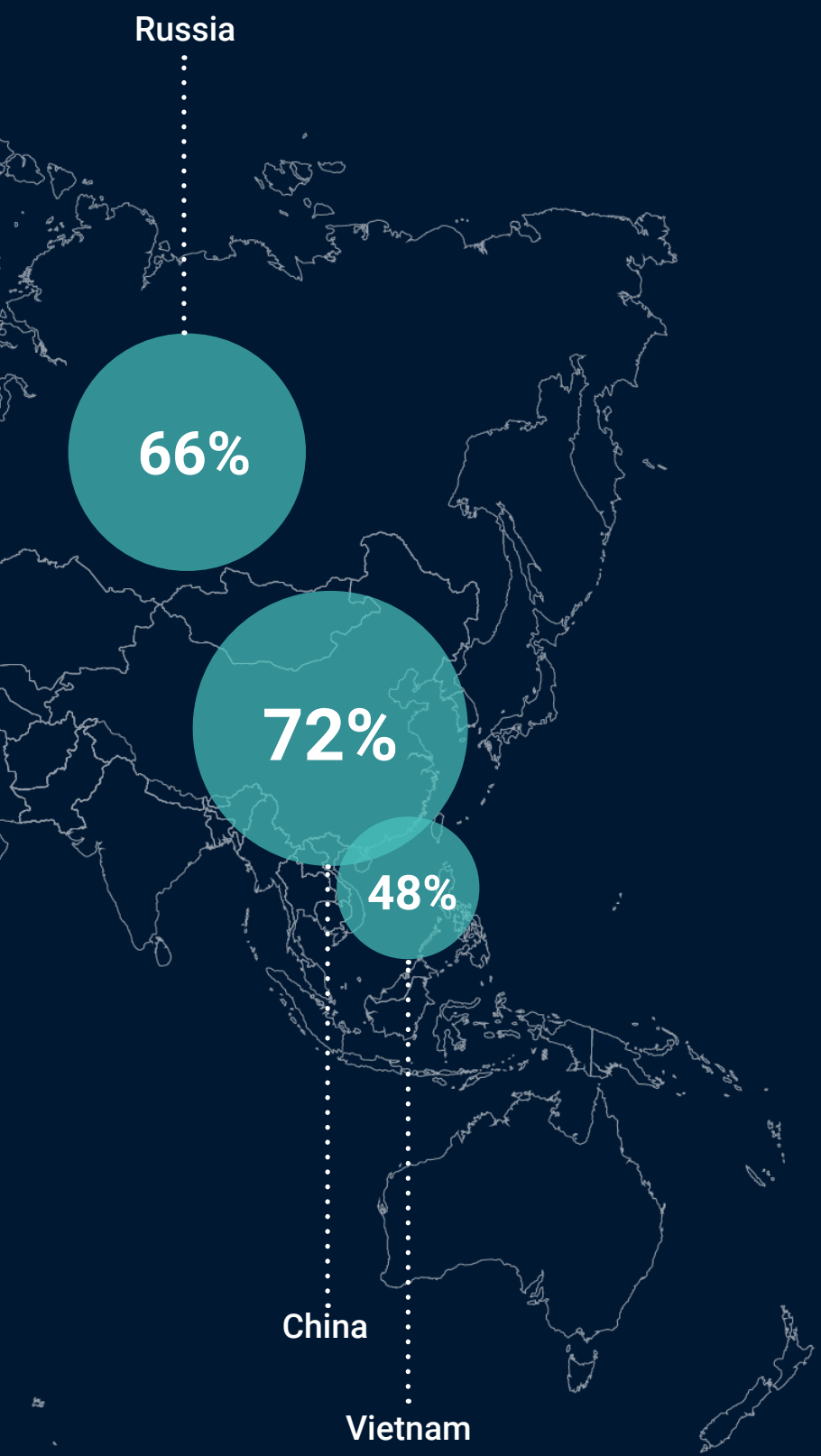
Across
UK and US

1. Report: Ransomware payouts and recovery costs went way up in 2023

2. Mandiant M-Trends 2023

Attack origin locations





Data highlights

- 53% of all attacks came from Russia or China
- 72% have been attacked by threats originating in China, 66% from Russia
- Malicious automated attacks on businesses from Russia have increased 82% in just two years - accounting for over 3/4 of all attack traffic from Europe
- Russian-sourced attacks have increased by 11% since sanctions were imposed in early 2022
- 72% of gaming and online streaming businesses reported attacks from Russia
- Vietnam is an outlier as third highest country of origin, with 48% seeing attacks from here despite the country accounting for just 2% of the population of Asia

Analysis

Russia and China - A permissible environment creating a launchpad for malicious automation

Are geopolitics behind malicious attacks on large enterprises? With over half our respondents saying they have been attacked from these two countries it may be a contributing factor, but it is not possible to attribute specific threat actors and motivations.

What cannot be disputed from the data, however, is that vast volumes of malicious automated traffic originates from infrastructure located in these territories. When overlaid on to global politics, and coupled with the fact that the businesses polled were exclusively in Western countries, it points towards a culture of permissibility. It might not be official policy, but neither is it cracked down on as it aligns with broader national goals.

Law enforcement and intelligence organizations in the US have made related points about both countries on several occasions. The FBI have called out[3] broad scale 'Chinese Economic Espionage' as well as the Director of CISA recently stating that cybercriminal gangs 'operate with relative impunity'[4] in states that provide them with safe harbor.

The Vietnamese outlier

Despite having less of a reputation for cyber-statecraft and playing a quieter role in global politics, nearly 48% of all businesses surveyed had been attacked in the past year by bots originating in Vietnam. Interestingly, this puts it third on the list of countries driving attacks against enterprises.

So why is this? This is likely a technological infrastructure issue - rather than a sign of Vietnam itself being a hotbed of adversarial activity. A boom in availability of cheap IoT devices in the country[5], everything from connected cameras to digital video recorders (DVRs), which started in 2017 made it easy for Vietnamese infrastructure to be exploited. Lacking security, these web-enabled devices are often co-opted into botnets and forced to launch attacks on large companies such as those analyzed.

Aware of the issue, Vietnamese authorities[6] have undertaken joint action; but businesses should consider that this still seems to be a common issue highlighted by the data.

3. "Responding Effectively to the Chinese Economic Espionage Threat" - FBI
4. "US cyber chiefs warn AI will help crooks, China develop nastier cyberattacks faster" - The Register
5. "How Vietnam Networks Unwittingly Expose Themselves To IoT Botnet Exploits" - Nexusguard
6. "What happens when a whole country tackles cyberthreats?" - Kaspersky

Academic perspective

Rob Black
Lecturer in Information Activities at Cranfield University

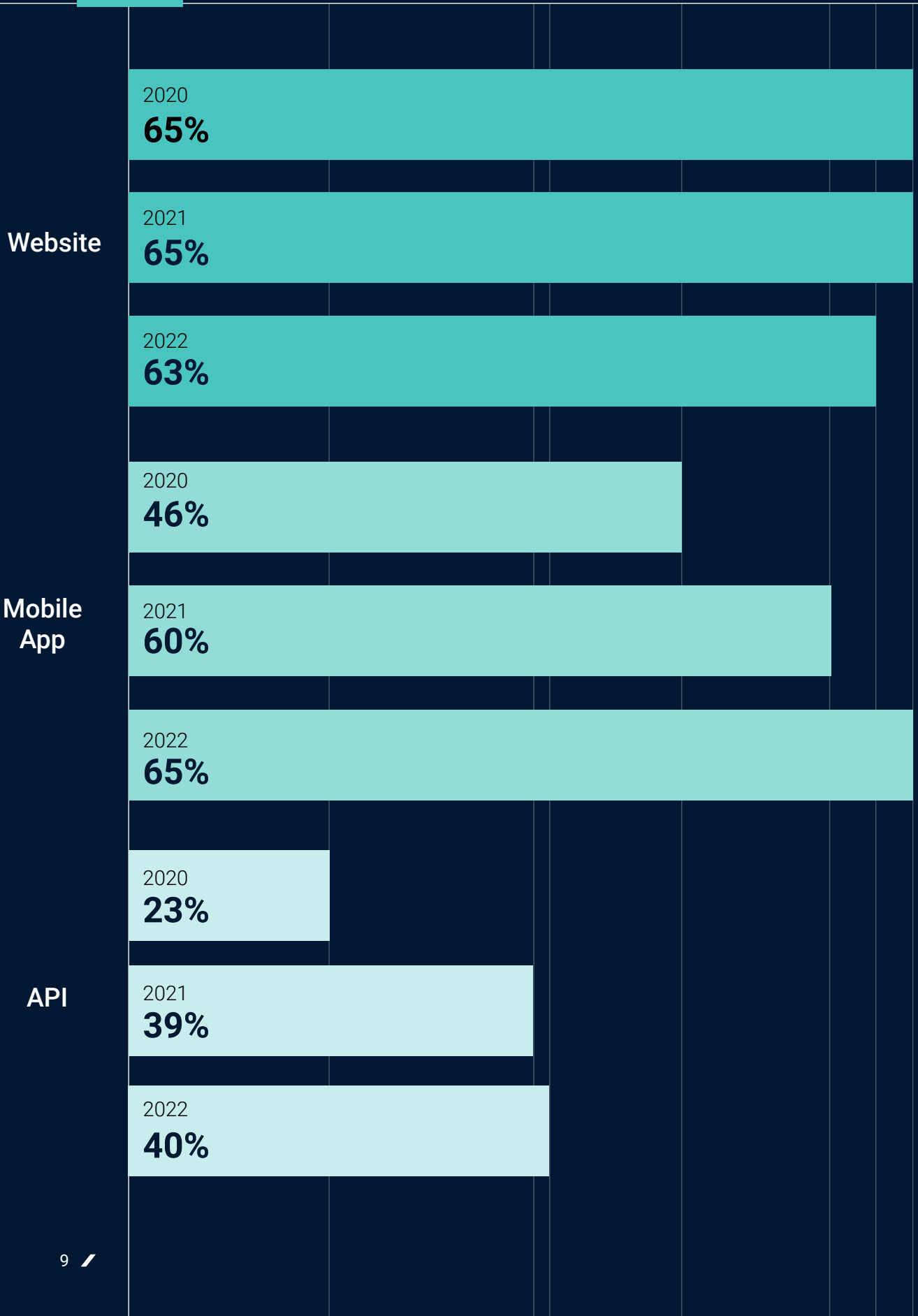
In today's age, conflict is no longer pursued solely through traditional military means. Instead, state actors are entering into a range of different forms of contest. More often than not these are enabled through rapid technological advancements, recognizing that we are no longer distinct nations separated by borders and seas, but instead are interconnected through networks, information flows and data.

Hybrid warfare and the desire to remain below the threshold of conventional warfare has encouraged states to innovate their means of causing harm and achieving influence. There is no domain in society unaffected by this and we are seeing hybrid warfare operate effectively through lawfare, economic coercion, the use of proxy actors and in many more formats. From the little green men operating in the Crimea in 2014 through to the use of misinformation to disrupt political processes in the US Presidential Election, malicious actors are pushing the limit in whichever domain they can, all enhanced by the cutting-edge capabilities that modern technology brings. They have recognized that strategically significant attacks that can only be associated with a state actor bring unwanted attention, and a coordinated response from the international community. Instead, a much more clever and effective means of influence is to seek approaches that remain under the radar of nation states and the international community, making it much more challenging for the community to agree how best to respond. They can degrade the effective operation of a society or a government's institutions, with little repercussion for their actions.

Economic coercion, in today's age, doesn't need to be the physical blockading of ports with gunboats. Instead, it can be the manipulation of markets, or the slow bleeding through the regular extraction of wealth from organizations who are not aligned with the hostile actors' aspirations and objectives. For a state, the challenges associated with proving any actor, or set of bots, are owned by a certain nation are one thing but the coordinated prevention of these subtle but deliberate actions across a multitude of potential targets, is near-on impossible. At this point, without a shot being fired, one can see how damage accrues over time - with the victim states having to operate in a way that does not cause tension with the aggressor state's aspirations.

Attack trends

Every surface is now a target



Data highlights

- Attack surface targeted by bots in the last year: 65% mobile, 63% website, 40% APIs
- Attacks on mobile applications surpassed attacks on websites for the first time in 2022
- Targeting of APIs rising at fastest rate – increase of 74% since 2020

Analysis

1

A broadening of the attack surface

Malicious automation is diversifying to take advantage of a swelling attack surface. As of 2023, mobile applications have become the predominant target over websites. APIs are also fast rising in popularity amongst threat actors – with the number of attacks reported by companies increasing by 74% since 2020. As recently as two years ago, most detected very little malicious automated activity within APIs. This has shifted in our most recent survey, with attackers increasingly exploiting the opportunity provided by unprotected APIs. Of organizations with over $5bn in revenues – 41% now see such attacks.

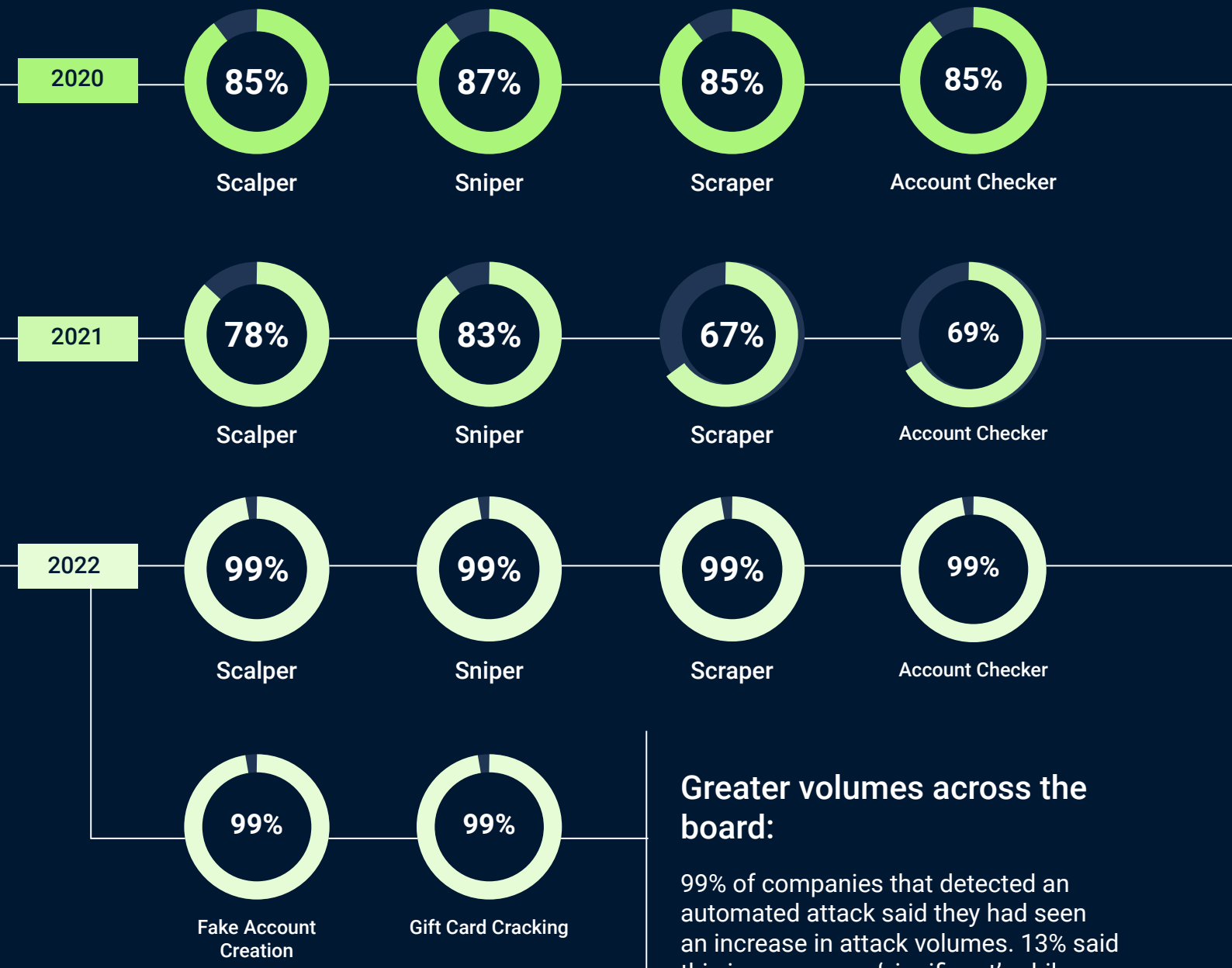
2

API attacks spread from financial services to other industries

Driven by emerging standards, financial services organizations were ahead of the curve with the utilization of APIs. Unfortunately, this resulted in 97% detecting bot attacks against these interfaces in our 2021 report. Seemingly, the financial services sector has responded with more sophisticated defenses, and now only 44% admit to being hit by the same threat. Conversely, as retailers, media organizations and telecommunications businesses have realized the value of using APIs, it seems to be presenting an opportunity for threat actors - with attacks increasing 40-fold over just two years. Ecommerce in particular stands out as the joint highest sector. We can speculate that this is a result of APIs being used to retrieve stock inventory used by the website or mobile app when a buyer selects an item. If left unprotected, attackers can bypass the website, going direct to the API and retrieving a retailer's entire stock details.

Threat volumes are rising

Increase seen in bot attacks over last year



Greater volumes across the board:

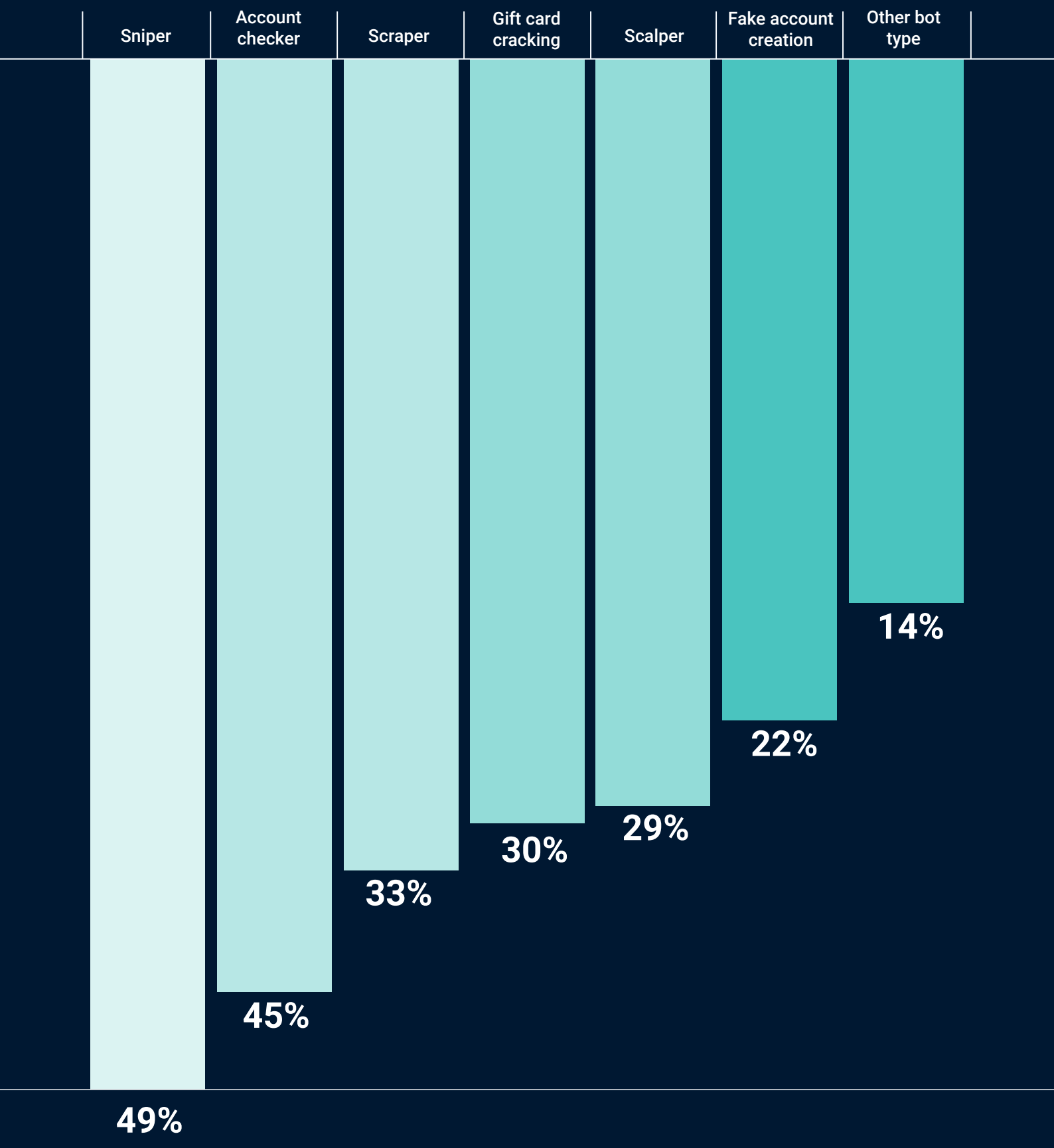
99% of companies that detected an automated attack said they had seen an increase in attack volumes. 13% said this increase was 'significant', while 61% saw a significant or moderate increase. At the larger end of the scale, 66% of companies earning $5bn+ in revenues reported a significant or moderate increase. Telecommunications and online entertainment specifically saw the greatest increases in attack volumes, with 66% reporting significant or moderate increases.

An increased variety of attacks leads to a greater impact on the business

Data Highlights

- Top three attack types: Sniping, Credential Stuffing, Scraping
- Nearly half of all organizations reported sniper bot attacks
- Over ¼ said they saw a significant increase in emerging gift card attacks

Types of bots that have attacked



Attack type analysis

Sniping

BLADE* Definition

Sniper bots (or “snipe bots”) are automated tools that monitor time-based activity and submit information at the very last moment, removing the opportunity for other people to respond to that action. The most common use of sniper bots is for last-second bidding on online auction sites.

Business impact

49% of businesses surveyed report being hit by sniping attacks. The highly dynamic pricing environments of financial services (56%) and travel (53%) make them the most likely to be exploited by sniper bot attacks.

Sniping can cause significant harm to businesses when applied at scale. This is evidenced by the fact that 91% of businesses with a turnover of $5bn or more say these attacks cause a greater than 10% drop in customer satisfaction, and 9% state it had a financial impact – draining 4.8% of online revenues.

Credential Stuffing

BLADE Definition

A credential stuffing bot is used to test previously leaked credentials to determine if they are valid on a target webservice or API. These bots validate sets of usernames and passwords against their target webservice or API by automating login attempts, allowing adversaries to test and validate credentials at mass scale.

Business impact

With international data protection organizations such as the ICO recently stating credential stuffing is ‘a significant and growing threat to personal information’ - it’s no surprise the financial services sector is most targeted by this form of malicious automation.

62% of financial services organizations admitted suffering such attacks, as opposed to the average of 45%. Across the board, half of all organizations questioned say between 3-10% of their customer accounts have been breached in this way in the last year, with 64% reporting a significant or moderate increase in attacks. The harm caused by credential stuffing attacks is growing, with 88% of businesses citing financial impacts this year, up 40% in just a year.

***The Business Logic Attack Definition (BLADE) Framework, is an open-source knowledge-base created to help cybersecurity professionals identify the phases, tactics and techniques used by adversaries to exploit weaknesses in the business logic of web facing systems (websites and APIs). To learn more about the BLADE Framework, visit www.bladeframework.org/**

Scraping

BLADE Definition

Web scraping is the use of bots to gather content or data from websites. Some scraper bots are beneficial to and welcomed by website administrators. However, some scraper bots, such as content and price scraper bots, can have malicious intentions and cause serious harm to businesses and their customers. A scraper bot could also be used to clone an entire website for use in a phishing campaign.

Business impact

Scraping has long been one of the most common bot attack types, with a third (33%) of all businesses suffering last year. This volumetric attack type puts a massive strain on website infrastructure, degrading UX for legitimate users and driving technical costs as it steals data.

This is underlined by the fact that 1/5th of all travel businesses admit that 10% of total web traffic was due to scraper bots stealing valuable data. The costs mount up in many sectors, for example 41% of eCommerce companies admit scrapers cost them over 5% of revenue last year.

Fake Account Creation

BLADE Definition

Fake account creation bots abuse the signup process of a webservice to create user accounts in bulk, using stolen or fake identities. These bots automate multiple signup requests, which can be spread out over long periods of time or using IP addresses from different geolocations to hide the fact that they are controlled by one person. Many advanced fake account creation bots can also bypass email, phone, and CAPTCHA verifications.

Business impact

Exploiting the fact that much of the value in online businesses now lies in their ability to automate the scaling of accounts, the research shows that attackers now create 3% of all new accounts for malicious purposes.

For high value sectors, this figure is greater, for example 30% of financial services businesses say 6-10% of accounts are fake. The cost adds up, ¼ of all businesses say the financial impact is over 6% of online revenue and 80% say it has caused a drop in customer satisfaction.

Scalping

BLADE Definition

Scalper bots use automated methods to purchase limited or high demand goods, such as event tickets. They are capable of buying many items at the same time and can complete the checkout process in a fraction of the time it would take any legitimate user.

Business impact

Scalper bots carry a danger of significant reputational damage for companies offering in-demand goods and services online. Of the nearly 1 in 3 (29%) online businesses hit by scalper bots, 93% noted an impact on customer satisfaction.

In 2022, 4% of all purchases were made by scalper bots and 62% of businesses reported that the challenge is increasing at a moderate or significant rate. The scalper bot problem is pernicious and costly, with nearly a quarter (24%) of businesses saying it has cost them over 6% of online revenue.

Gift Card Fraud

BLADE Definition

A gift carding bot is used by adversaries to validate stolen gift cards or enumerate gift card codes for subsequent use or sale.

Business impact

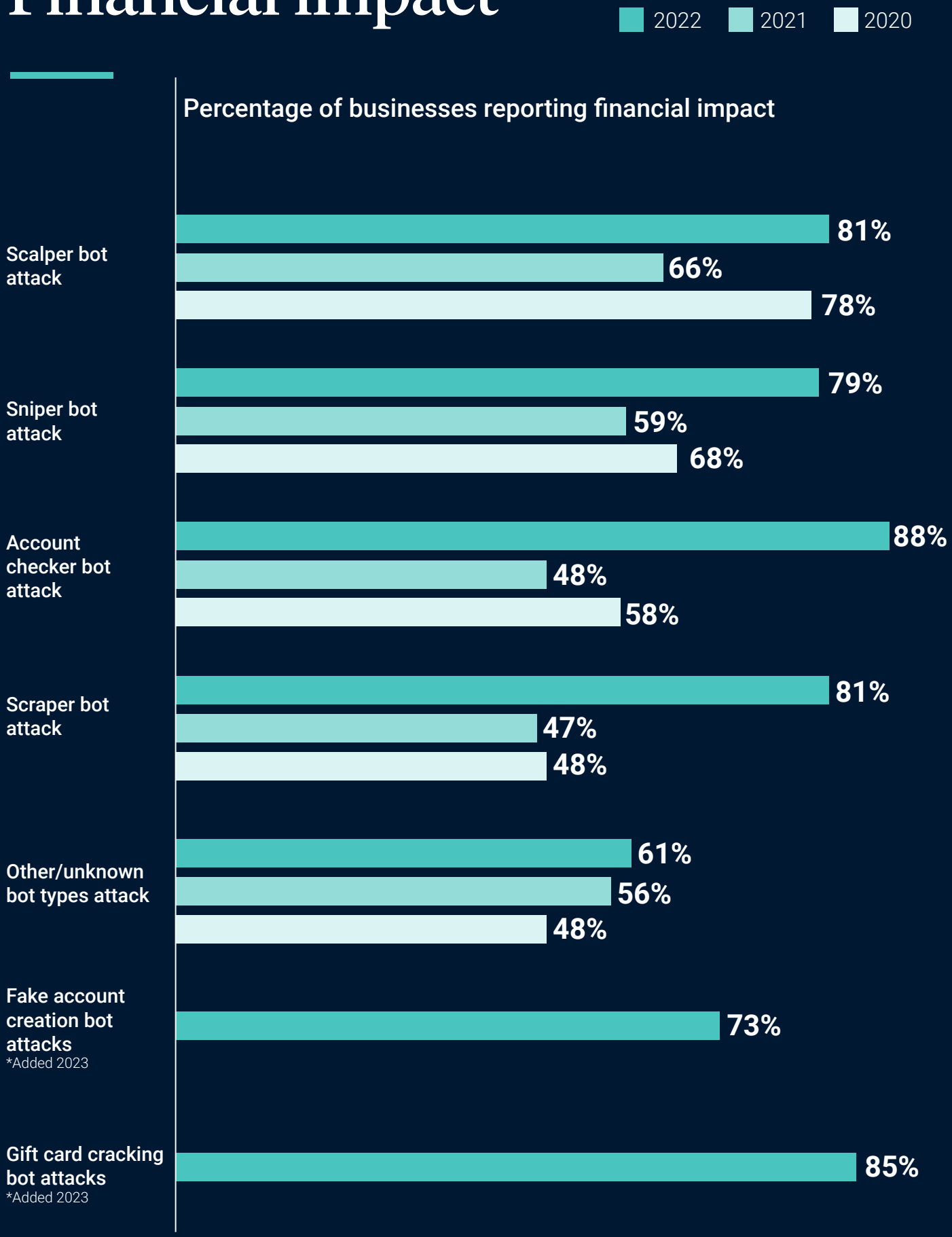
An emerging automated threat used by attackers to drain value, the businesses researched said one in 20 gift card transactions in the last year were fraudulent. Ecommerce organizations were the focus of gift card fraud attacks, with 44% saying they were targeted in the last year. The cumulative business impact is significant – costing 4.7% of online revenue on average as customers are reimbursed and fraudulently acquired stock is replaced. At scale, the compound effect costs large companies hundreds of millions of dollars every year, as well as reputational damage.

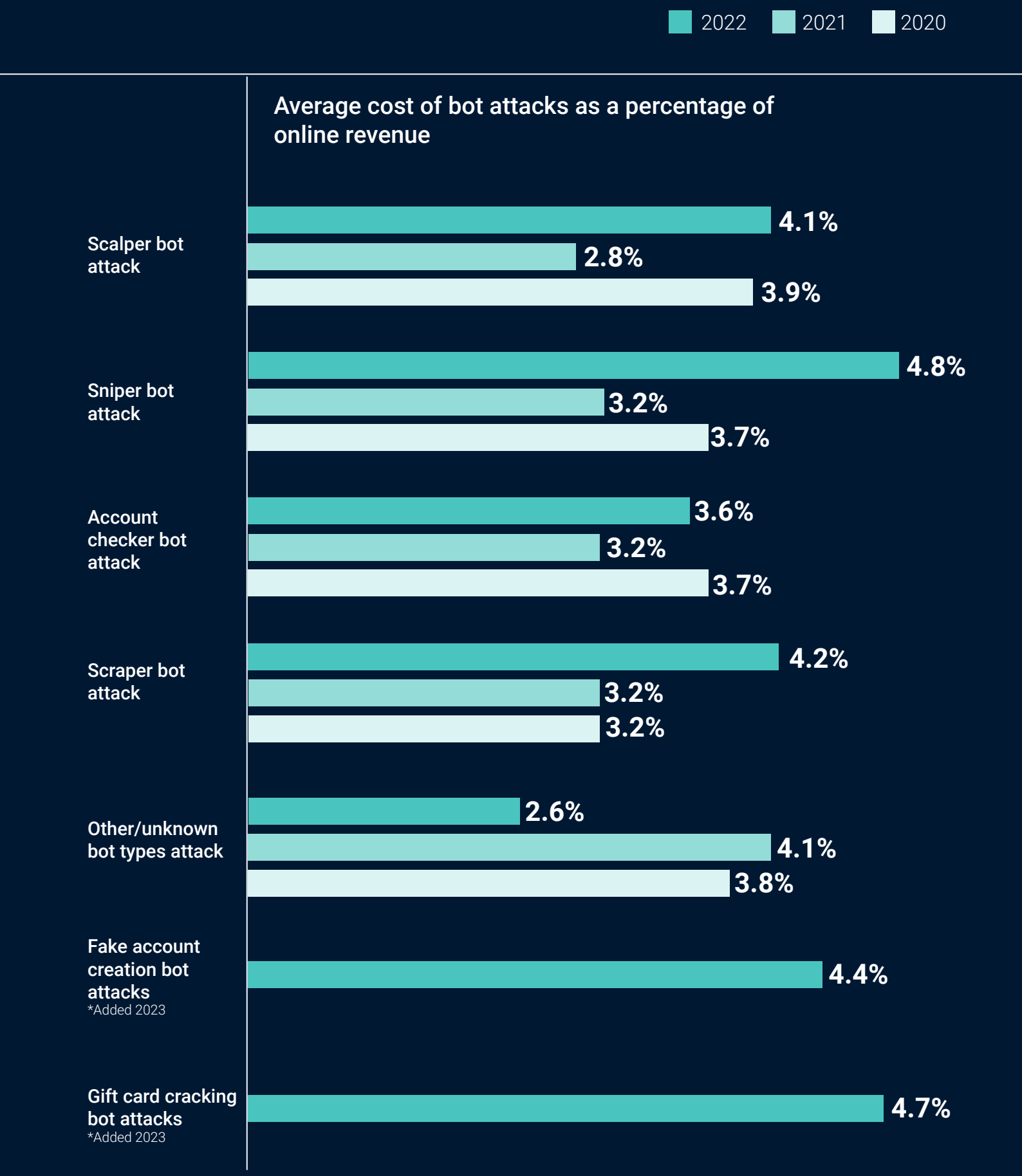
Business impact

Security teams at online businesses often know they have a malicious automation problem, but quantifying impact is difficult. Traditional CISO risk equations, based on calculating the probability of singular disruption to a tangible business asset, struggle with a threat that continually drains value in small, often invisible, increments.

	Traditional cyberattacks	Malicious automation
Presents as	Definable incident	Countless small attacks
Value targeted	Clear: • Ransom demand • Data theft / sale • Hacktivism	Opaque: • Revenue leakage • Customer churn • Reputational damage • Infrastructure cost
Discovery	Focused - cybersecurity teams	Distributed across functions
Financial harm	One-off, evident, exceptional	Lost revenues, customers and Opex accumulates over time
Reputational harm	High-profile, crisis process defined	Both high profile / short and long term / ongoing
Board engagement	High, accepted risk	Low, lesser known

Financial impact




2022
2021
2020
Average cost of bot attacks as a percentage of online revenue
Scalper bot attack
4.1%
2.8%
3.9%
Sniper bot attack
4.8%
3.2%
3.7%
Account checker bot attack
3.6%
3.2%
3.7%
Scraper bot attack
4.2%
3.2%
3.2%
Other/unknown bot types attack
2.6%
4.1%
3.8%
Fake account creation bot attacks
*Added 2023
4.4%
Gift card cracking bot attacks
*Added 2023
4.7%

Analysis

The data shows a growing awareness of the harm inflicted by bots, with 81% saying their business has been impacted financially, a 47% increase on last year's total.

To quantify the scale of this impact, the business analyzed admitted that automated attacks cost, on average, 4.3% of online revenues. Context is required to truly understand the sheer scale of accumulated impact here. With average online revenues of $1.9bn - every company estimates it is losing $85.6m each, per year, to bots. To put this in perspective, this is the equivalent of:

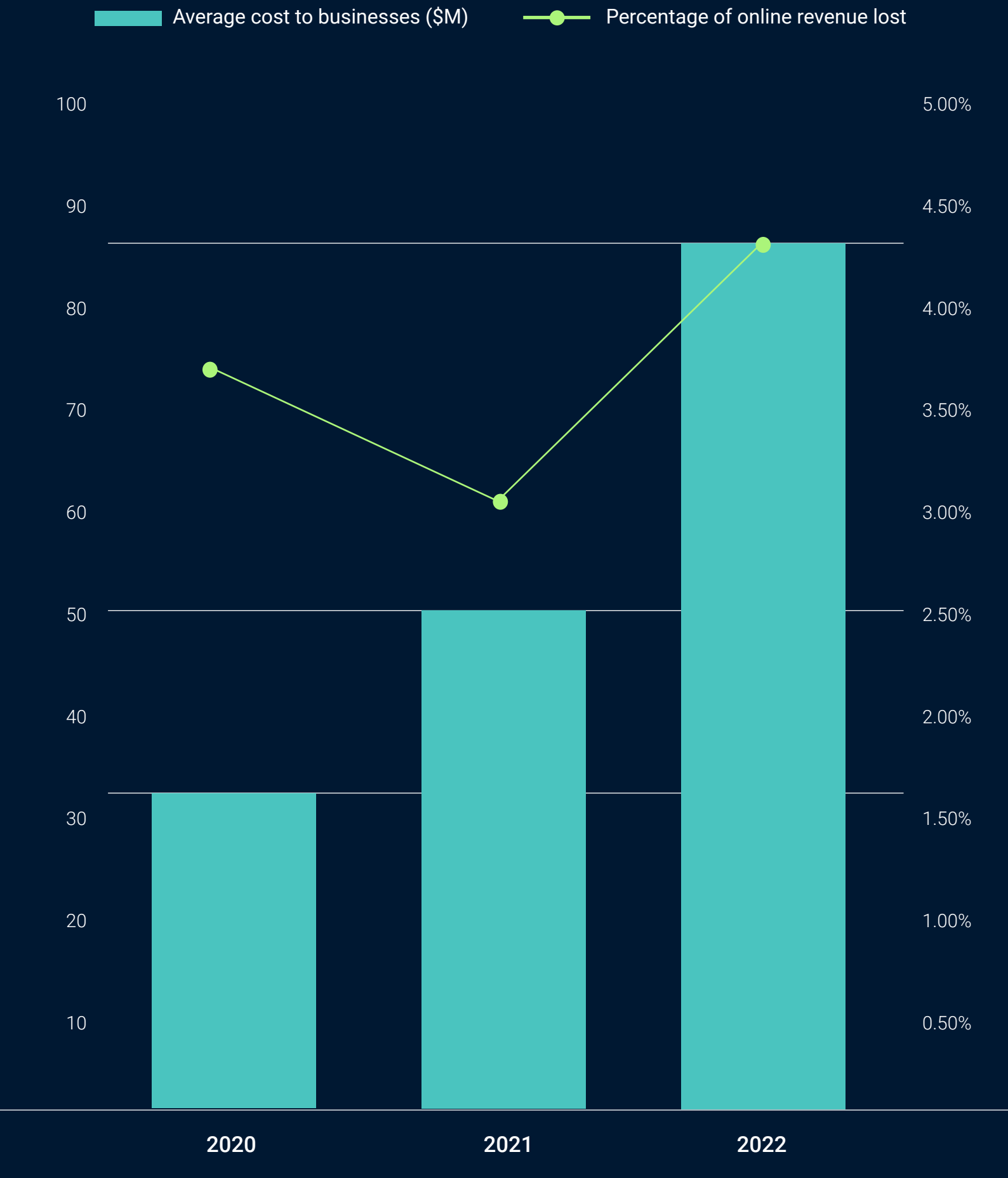
- The 8th largest GDP fine ever issued[7], per company, per year
- 57 average ransomware demands[8] ($1.5m)
- 19x more than the average cost of a data breach[9]

7. https://www.enforcementtracker.com/

8."Report: Ransomware payouts and recovery costs went way up in 2023" - SC Media

9 Cost of a Data Breach Report 2023" - IBM.

Financial impact is growing:



Where companies accrue financial damage from bots

As highlighted, the persistence and presence of malicious automation on the web attack surface creates financial damage over time.

Examples borne out by the data include:

Sniping

9% of the highest turnover companies said it impacted at least $260m of their online revenues per year

Scalping

45% of companies with online revenues of $2.6bn said it cost more than 5% of online revenues

Scraping

30% of companies over $2.6bn in online turnover say it cost over 5% of online revenues

Credential Stuffing

2% of security leaders at the highest turnover organizations said it cost more than 10% of online revenues

Fake Account Creation

Over ¼ of smaller organizations with an online run rate of just over $100m said it caused at least $6.2m to drain away annually

Gift Card Fraud

38% of organizations with total revenues over $5bn, say the cost is greater than 5% of total online revenues - or at least $130m.

Reputational impacts with customers

Alongside financial impacts, the data shows companies' reputations with their customers are also being corroded by malicious automation. On average, 88% of the businesses surveyed indicated bots have impacted customer satisfaction. 22% of these said customer satisfaction had dropped 6% or more as a direct result.

"Given the media's interest in scalper bots and a high-profile appearance in Congress following the commotion surrounding the Taylor Swift Eras tour ticket release, it is perhaps no surprise that 93% of businesses identified scalping as a drain on reputation, the most impactful attack type. This was followed closely by credential stuffing – which can be a particularly 'noisy' attack for users, either locking them out after multiple failed attempts or forcing them to take arduous remediation actions."

Cyril Noel-Tagoe
Principal Security Researcher at Netacea

Mitigations

Big gaps in detection and response

Length of time before realising attack
(Average months)

Scraper	4.02
Fake account creation	3.97
Account checker	3.93
Sniper	3.88
Scalper	3.44
Gift card cracking	3.40

The research highlights poor detection times across the board, which likely contribute significantly to the attritive business impact of bots. Worryingly, speed of detection and remediation times are measured in months, not days or weeks.

The average dwell time for a malicious automated attack on the web attack surface is 4 months. In fact, nearly every single organization researched (97%) said it takes over a month to respond to malicious automated attacks. This is at odds with accepted best practice when detecting attacks in other areas of the technical environment. For example, Mandiant's recent M-Trends report states that average dwell times globally are down to just 16 days[1] and IBM's Cost of a Data Breach report states that breaches identified within 200 days are 26.5% less costly than breaches with a lifecycle greater than 200 days.[2]

Detection and response times

Sniping

- Nearly half take between 4-6 months to detect
- Ecommerce moves fastest with a 55% detection rate in 2-3 months

Scraping

- Longest average time to detect at 4.02 months
- 10% of scraping attacks aren't detected until 7-9 months after they begin

Scalping

- Over 1/3 of companies take 4 - 6 months to detect
- ½ of all financial services companies don't detect for 4-6 months

Fake Account Creation

- 55% of companies exceeded the average 4-month detection time
- 60% of the highest revenue businesses detect slower than average time

Gift Card Fraud

- Travel sector has the slowest detection times with 70% taking longer than the average organization across other sectors
- Largest companies detect the fastest - with 89% identifying attacks in less than 4 months

Credential Stuffing

- 45% take between 4-6 months to detect attacks
- 40% of financial services companies don't detect for 4-6 months

10. Mandiant M-Trends 2023
11. Cost of a Data Breach Report 2022, IBM Security

Lagging as a strategic risk priority

How much of a concern were bots in 2022 compared to 2021?

	Sector				
	Travel	Online entertainment	eCommerce	Financial services	Telecoms
Scalper	47%	56%	40%	71%	48%
Sniper	36%	37%	49%	38%	42%
Account checker	44%	52%	52%	34%	45%
Scraper	58%	59%	67%	42%	68%
Fake account creation	73%	70%	71%	67%	78%
Gift card cracking	62%	68%	56%	75%	62%
Other bot type	79%	83%	77%	75%	78%

Andy Still
Co-Founder, Netacea

A need for action

Overall, the data points towards a highly impactful and increasing threat that is capitalizing on slow response times and a lack of priority in overall security posture.

The huge levels of financial damage, as proven by this research, should secure its place in board level discussions alongside ransomware attacks and data breaches. However, the incremental nature of monetary, reputational and operational cost, and the fact this is spread across departments, means impact hides amongst the numbers. Security leaders must link attack data to business impact to stop bots being buried in the cost of doing business. Only this way will they glean the C-suite support and resources necessary to address the problem.

Accessing effective resources is critical to stopping the growing threat to business posed by malicious automation. Attackers are exploiting an expanding web attack surface, while the increasing sophistication of AI presents significant opportunities for attackers to amp up the volume and complexity of attacks. From a wider perspective there also seems to be little desire for regulators in Western nations to act, or for malevolent infrastructure to be removed in countries with contradictory world views.

Without sufficiently intelligent AI-driven defenses in place, companies risk becoming complacent about the accelerating damage caused by malicious automation to their bottom-line. This is a costly lesson for many who invest in inferior solutions. There is hope, however, as Gartner recently pointed out this is a market set to reach maturity over the next two years, no doubt driven by some of the factors outlined above.[10]

Action sits squarely with security leaders for whom taking the first step requires acknowledging the scale of the problem. Without this, companies will continue to suffer death by a billion bots.

12. "Netacea named as a Sample Vendor in Gartner® Hype Cycle™ for Application Security 2023" - Netacea

NETACEA

Take the next step

Stop bots bleeding your business:

1. Understand more about malicious automation with our threat reports, webinars, blogs and podcasts.

   View the Resources

2. Fix the problem of sophisticated bots with the Netacea platform which combines edge computed analysis with advanced malicious detection and response for 30 times better results.

   Book Your Demo

About Netacea

Netacea prevents sophisticated, high-volume, bot attacks that drain value from online businesses. Situated on the far edge of technical infrastructure, the platform combines unrivalled visibility of all traffic across APIs, applications and websites with evolved detection, response and threat intelligence capabilities. The result is more effective automated protection for highly trafficked businesses.