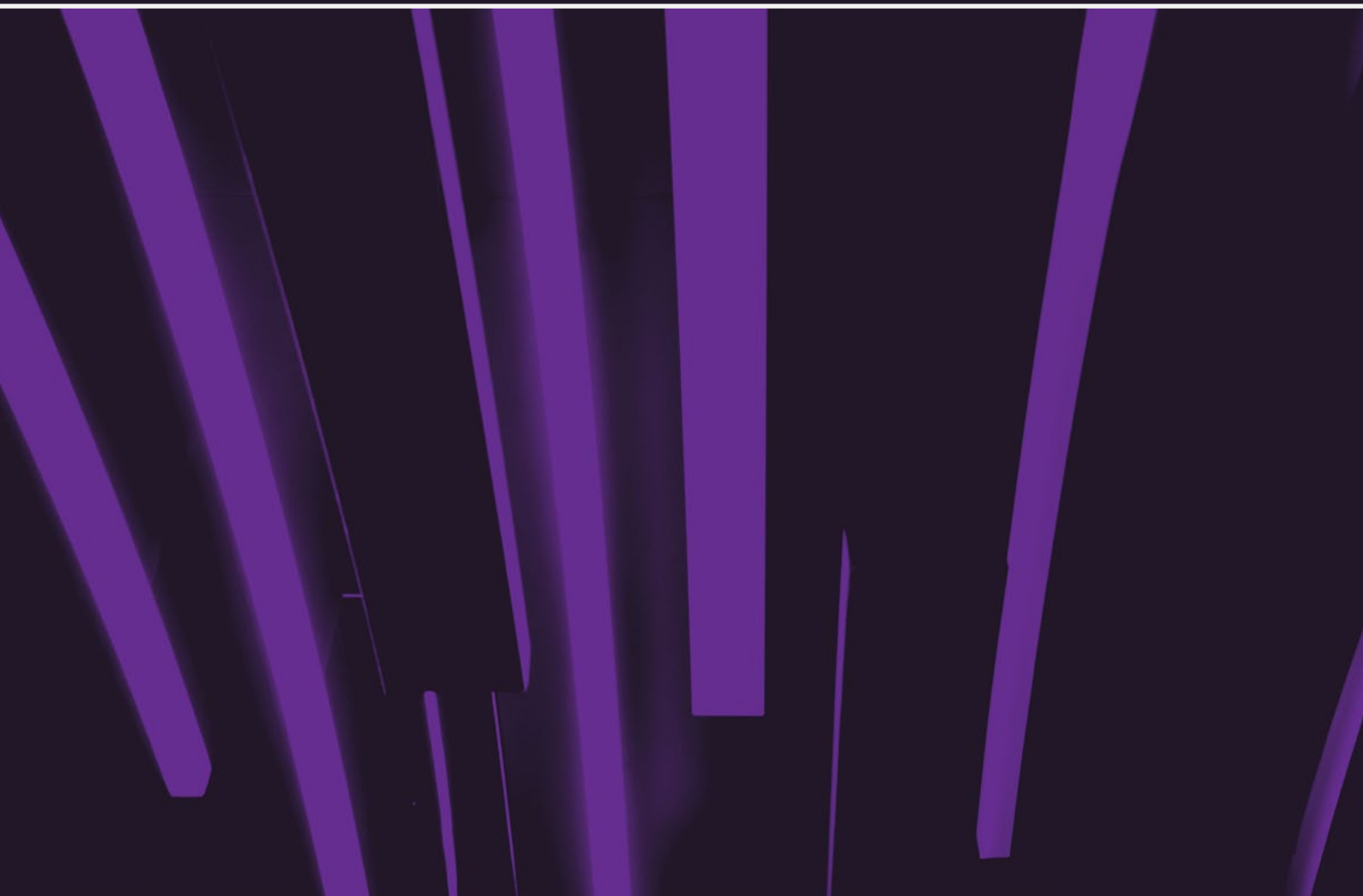
Veracity Trust Network

Demystifying The Web Bot Threat:

A COMPREHENSIVE GUIDE VERSION 1 - NOVEMBER 2023



Veracity Trust Network

01 Introduction

Bots have been an integral part of the digital landscape since the beginning of the World Wide Web.

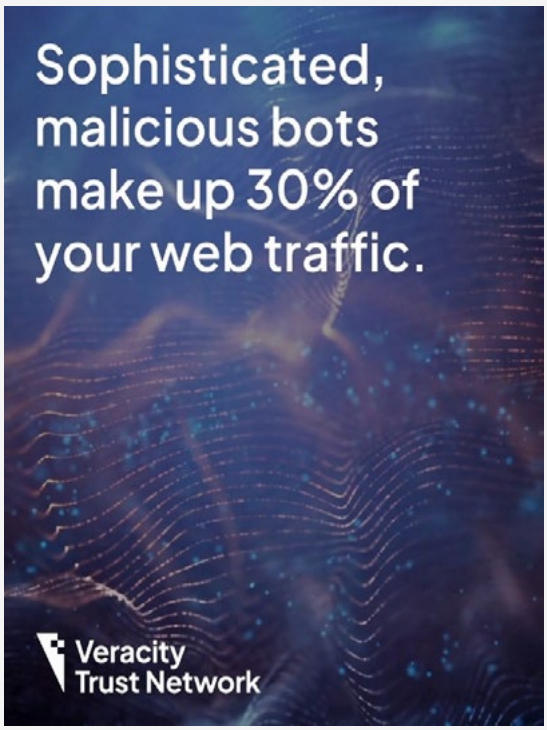
Many of them are harmless, they help us order food, they're used in apps to support customer service, and a lot of them exist to help the internet to work as it should do.

Google and other search engines use bots to crawl the web and index web pages for their search engines.

Ad Blocking bots help keep website visitors from being bombarded with unwanted ads and site monitoring bots are used to monitor website metrics, such as uptime or page speed.

But with the rise in the internet being at the heart of so many critical business functions, comes the rise of malicious bots deliberately programmed to act in bad faith.

The Growing Threat: Bots in the Digital Landscape



When 30% of internet traffic on any given day is made up of bots, according to our own research, there's a growing chance quite a few of those will be malicious, seeking access to websites and data through exploiting vulnerabilities and shortfalls in bot mitigation.

This can include:

- Using bots to crawl web pages and steal content;
- Serving spam, scraping information, and generating fake ad impressions in online marketing campaigns;
- Driving bad ad placements in fraudulent programmatic platforms;
- Filling out forms with fake information to create bad leads;
- Spamming your organisation's contact or survey forms with bad messages—which can keep you from responding to genuine inquiries;
- Gathering up-to-date information from websites to aid more convincing phishing & vishing campaigns;
- Posting fraudulent reviews on websites to make products and services look better or worse than they actually are to potential customers.

Malicious bots can be an even bigger threat than just muddying the waters of your digital marketing campaigns or affecting your online presence.

Even the smallest breach may cost upwards of $200k to fix, with more complex and comprehensive breaches costing millions.

Besides potentially substantial direct costs, such breaches can put an organisation at the risk of violation of local data protection violations, such as GDPR or the California Privacy Rights Act. It can also lead to losing customers' hard-earned trust.

According to an IBM report - the Cost of Data Breaches - nearly half of consumers surveyed said they had stopped doing business with a company known to have experienced data loss through a cybercrime event.

This is alarming news when coupled with the global average cost of a data breach reached an all-time high of $4.45 million for the organisations surveyed independently by the Ponemon Institute on behalf of IBM.

This represents a 2.3% increase from the 2022 average cost of $4.24 million. Since 2020, when the average total cost of a data breach was $3.86 million, the average total cost has increased 15.3%.

The top five countries and regions for the highest average cost of a data breach were: the US at $9.48 million, the Middle East at $8.07 million, Canada at $5.13 million, Germany at $4.67 million, and Japan at $4.52 million.

The UK saw a significant drop in average cost at $4.21 million -- down 16.6% from last year -- placing just outside of the top five.

From client-side attacks that steal sensitive data, to bots that leverage it to commit fraud - as financial incentives grow and attack costs lower, the risk to all organisations and their brand website increases.

According to the UK Cyber security breaches survey 2023, 11% of businesses and 8% of charities experienced cybercrime in the past 12 months, rising to 26% of medium business, 37% of large business and 25% of high-income charities.

This means of the 32% of businesses and 24% of charities that identified any cyber security breaches or attacks, around a third of each ended up being victims of cybercrime.

Attacks from bad bots are often the first indicator of fraudulent activity targeting your brand website.

83%
of organisations studied have had more than one data breach

60%
of organisations' breaches led to increases in prices passed on to customers

79%
of critical infrastructure organisations didn't deploy a zero trust architecture

19%
of breaches occurred because of a compromise at a business partner

45%
of the breaches were cloud-based

Veracity Trust Network

The Vulnerabilities: Why your website can be a risk factor

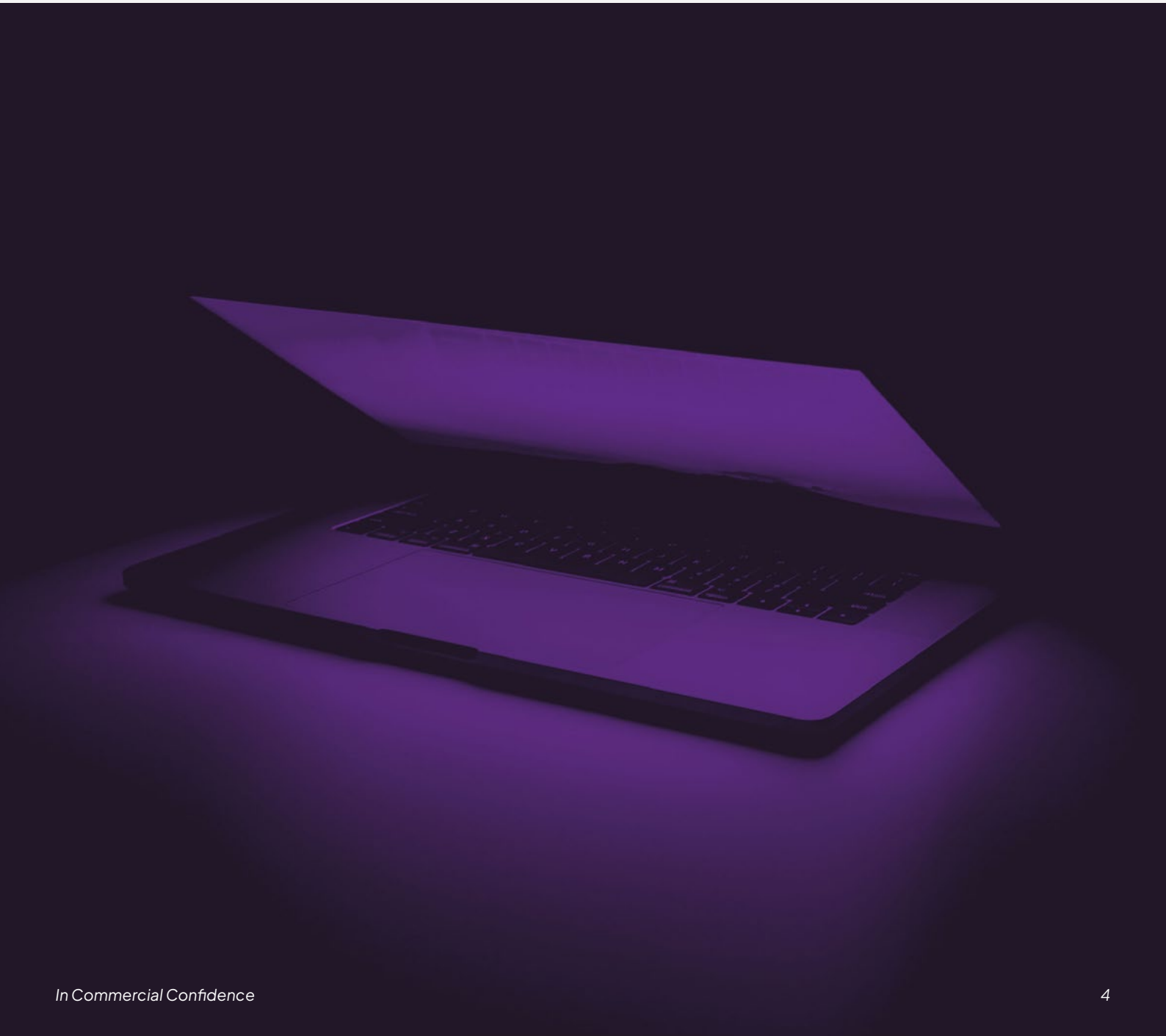
Your website is one of the most important assets you will own as a business, but it can also be exploited as a vulnerability, causing untold damage both financially and to your brand reputation.

A website vulnerability is a software code flaw or bug, system misconfiguration, or some other weakness in the website or web application or in its components and processes.

This can come in a variety of ways, from over-the-top surface level bots which are used to validate stolen user credentials or to steal credit card information (which is then sold on the dark web) or scraping proprietary data which is used to gain a competitive edge in the marketplace.

Out of date website plug-ins, insecure contact forms, basic log ins which don't use Two Factor Authentication, websites which still use default Administrator logins/passwords, open ports, are all potential exploit openings which can be used by hackers to gain access to your business - and your client - data.

Organisations of all shapes and sizes must ensure that they are able to detect and stop fraudulent activity on their brand websites and applications.



Veracity Trust Network

02
Understanding the Bot Problem

To highlight the size of the bot problem, there were in excess of 57 billion bot-initiated attacks in human-initiated financial services processes in 2021 (this is believed to be an underestimate. Source: Help Net Security), growing at 41% per year.

Almost half of all internet traffic in 2022 came from bots

and 30% of that half was generated by malicious bots – up from 20.4% in 2018.

The cost of bot traffic – as measured through digital ad fraud

is projected by Statista to reach $100 billion in 2023.

If it were measured as a country, cybercrime - which was predicted to inflict damages totalling $6 trillion globally in 2021

would be the world's third-largest economy after the US and China.

Types of Bots: Account takeover, Scrapers, Spambots, botnets and Beyond

Essentially, a bot is an automated software application that performs repetitive tasks across a network and follows instructions to imitate human behaviour - but in a much faster and more accurate fashion.

Malicious bots perform activities that create security risks for any business or organisation. They can disrupt operations, create unfair disadvantages, send out unwanted emails or attempt unauthorised access to sensitive data.

The most dangerous types include Account takeover, Scrapers, Spambots, and Scalpers.

Account Takeover Bots

Account Takeover is a form of identity theft and fraud. It happens when someone gains control over an account by using the customer's credentials and makes unauthorised transactions on their behalf.

Scrapers

Scraper bots are tools or pieces of code used to extract data from web pages. Web scraping software may directly access the World Wide Web using the Hypertext Transfer Protocol or a web browser.

It is a form of copying in which specific data is gathered and copied from the web, typically into a central local database or spreadsheet, for later retrieval or analysis.

Spambots

A spambot is a computer program designed to assist in the sending of spam. Spambots usually create accounts and send spam messages with them.

Scalpers

Scalper bots automate the entire checkout process. In less than a few seconds, they can login, add items to cart, enter personal details and credit card information, and complete the purchase.

Veracity Trust Network

Why Bots Are a Serious Concern

The National Association of Corporate Directors (NACD) noted the importance of cyber risk quantification in its 2023 Director's Handbook on Cyber-Risk Oversight.

The NACD included in its citations a book that Douglas W. Hubbard and Rich Seiersen, Chief Risk Officer of Resilience, wrote: "*How to Measure Anything in Cybersecurity Risk*".

According to Seiersen: "*One of the worst questions to be asked as a CISO in a boardroom is, "Are we secure?" This is because it's an intangible status which is difficult to qualify.*

He added: "*What boards should ask instead, is* ***'are we resilient to material losses?'*** *When boards frame the question like this, they are seeking an answer that extends beyond the CISO to include the Chief Financial Officer and CRO."*

What is needed is a strategic, grounded approach to mitigating and transferring cyber risk, and that starts with collaboration in quantifying the risk.

Allowing bad bots to access systems can be very expensive for organisations in several ways, including:

Loss of revenue associated with brand website downtime and/or performance degradation

Increased operational expense including infrastructure costs, authentication expenses, and the people cost of the time spent on bot mitigation

Regulatory penalties such as the huge fines imposed on organisations for breaches of, for example, GDPR or AML regulations

The intangible (and sometimes tangible) damage to brand reputation resulting from negative publicity and loss of customer confidence

Any business which handles sensitive customer information, for example, legal firms, eCommerce sites, insurance, financial institutions, are at high risk of being targeted by malicious bots.

Online marketplaces, travel and hospitality companies, gaming websites, healthcare providers and public sector organisations are also vulnerable to bot attacks because of the wealth of data they store.

But no business sector is immune.

Real-World Bot Attack Examples

One of the most famous bot attacks in recent years is Methbot. This advertising scam involved a group of Russian hackers building a click-fraud machine that stole up to $5 million daily from top advertisers and publishers.

High profile UK data breaches in the last couple of years, including the Cambridge Analytica scandal, and those which impacted Virgin Media and Mumsnet, have led to growing worries across all industries.

However, there have also been a spate of ransomware attacks in 2023, including the Movelt hack.

This saw threats being issued to big name companies including the BBC, Royal Mail, outsourcing firm Capita, Boots, Aer Lingus and British Airways.

In the UK, the payroll services provider Zellis was one of the companies affected and it said data from eight of its client firms had been stolen.

In September it was also revealed that leading UK charities including the RSPCA, Dogs Trust, Battersea Dogs & Cats Home and Friends of the Earth, had been caught up in a cyber-attack on a third-party supplier.

The company, About Loyalty, which carries out supporter surveys for more than 40 charities, said hackers had accessed personal information via a sub-contractor that handled data on its behalf.

While no financial data has been taken, the information that has been lost could be used by scammers to send out fake emails that have been mocked up to look like legitimate fundraising appeals.

Other big names that have been victims of hacking this year include The Electoral Commission, Police Service Northern Ireland and a firm in Stockport which makes ID cards for Greater Manchester Police (GMP) that was targeted in a ransomware attack in August, leaving the police force's data exposed.

Another recent bot, Qakbot malware (also known as 'Qbot' and 'Pinkslipbot') infected more than 700,000 computers globally via spam emails.

An operation by the FBI and the US DoJ, saw the seizure of Qakbot's infrastructure in the US and across Europe earlier this year in August, with the NCA ensuring UK servers were taken offline.

The action represented the largest US-led financial and technical disruption of a botnet infrastructure leveraged by cybercriminals to commit ransomware, financial fraud, and other cyber-enabled criminal activity.

Veracity Trust Network

03
Unveiling The Coverage Gap

According to Forrester Consulting's State Of Online Fraud And Bot Management, 78% of organisations are using denial-of-service (DDoS) protection, web application firewall (WAF), and/or content delivery networks (CDNs) to manage bots but only 19% have a full bot management system in place.

Regardless of what kind of bot traffic you attempt to mitigate, there are three key steps in the process:

1. **Identifying bot traffic:** You need to be able to identify a malicious bot from a human user in order to then implement filters to prevent it occurring again;
2. **Assessing bot behaviour:** This is where understanding the difference between good and malicious bots is necessary;
3. **Blocking damaging bots:** Once identified, you need to be able to prevent malicious bots from accessing your website or data.

According to Verizon's 2023 Data Breach Investigations Report (DBIR), 74% of all breaches involve the human element.

Employees are often the first line of defence against cyberattacks. But without proper training, they can also be the weakest link.

The Verizon report also found 83% of breaches involved External actors, and the primary motivation for attacks continue to be overwhelmingly financially driven at 95% of breaches.

The three primary ways in which attackers access an organisation are stolen credentials, phishing and exploitation of vulnerabilities.

The UK Government's Cyber Security Breaches Survey for 2022 found that of the 39% of UK businesses who identified a cyber attack, the most common threat vector was phishing attempts (83%).

The Singapore Cyber Landscape 2022 report noted that phishing attacks more than doubled from 2021 to 8,500 reports in 2021 in Singapore alone.

Bot mitigation is an ongoing effort and should be a priority for the C Suite. Periodic third-party audits and vulnerability assessments provide an external perspective on security posture and help identify gaps, risks, and opportunities to address any shortcomings.

Traditional Security Measures vs Advanced Bots

There are shortcomings in the most common and accepted bot mitigation technologies, especially when it comes to advanced bots.

One perfect example of this is solutions offering CAPTCHA challenges, as these are not only ineffective at detecting and stopping automated attacks, but they bring an added frustration to a human end user when they give repeated errors.

This leads to frustrated potential clients and a negative impact on sales. In addition, fraudsters and criminal gangs also use *"human farms"* - people being paid miniscule amounts to log onto the internet and act as genuine buyers or users - to bypass CAPTCHA protocols.

This was demonstrated perfectly during the recent PS5 and Xbox Series X console launches which pitted

human buyers against bots owned and operated by scalpers on retailer websites.

Bots are getting cleverer, and as a result account takeover attacks, including attacks against APIs, are increasing.

These are growing because they are relatively under-protected and easier to attack with automation because they are made for automation. Brute force or credential stuffing is the primary method used to force an account takeover.

Cybercriminals keep trying permutations and combinations of credentials until they find one that succeeds.

Bot mitigation approaches that are based on observations from historical and contextual data, which then implements IP blocking protocols, can also suffer from inaccuracies and end up blocking legitimate human users who may surf the web outside of "*normal*" hours, i.e. late-night shoppers.

Blind Spots in Current Enterprise Defences

A joint advisory from agencies in the UK, Australia, Canada, New Zealand, and the USA has revealed the top 12 cyber vulnerabilities that were routinely exploited last year.

In 2022, malicious cyber actors exploited older software vulnerabilities more frequently than recently disclosed vulnerabilities and targeted unpatched, internet-facing systems.

Proof of concept (PoC) code was publicly available for many of the software vulnerabilities or vulnerability chains, likely facilitating exploitation by a broader range of malicious cyber actors.

The allies are warning organisations about the importance of updating systems after malicious cyber attackers were seen routinely targeting older software vulnerabilities in 2022.

More than half of the top vulnerabilities listed for 2022 also appeared on the previous year's list.

This highlights how malicious cyber actors target previously disclosed flaws in internet-facing systems – despite security updates being available to fix them.

Jonathon Ellison, NCSC Director of Resilience and Future Technology, said: "*To bolster resilience, we encourage organisations to apply all security updates promptly and call on software vendors to ensure security is at the core of their product design to help shift the burden of responsibility away from consumers.*"

The Three Main Ways your Website can be Vulnerable to Attack

Client-side attacks

This is when your web site host server has been breached and is then used to target your web browser.

There are six main types:

1. SQL Injections;
2. Cross-Site Scripting (XSS);
3. Command Injections;
4. File Inclusion (LFI/RFI);
5. Cross-Site Request Forgery (CSRF);
6. Security Misconfigurations.

Server-side vulnerabilities

Cybercriminals may start by identifying your website's server type, software and operating system. Once they know what's going on behind the scenes, they can exploit open ports, default configurations and access the server folders.

They are looking for:

- Outdated WordPress plug-ins;
- Outdated Contact Forms;
- Open Ports;
- Unnecessary services;
- Websites that still have default keys and passwords in place.

Veracity Trust Network

Direct cyber-attacks

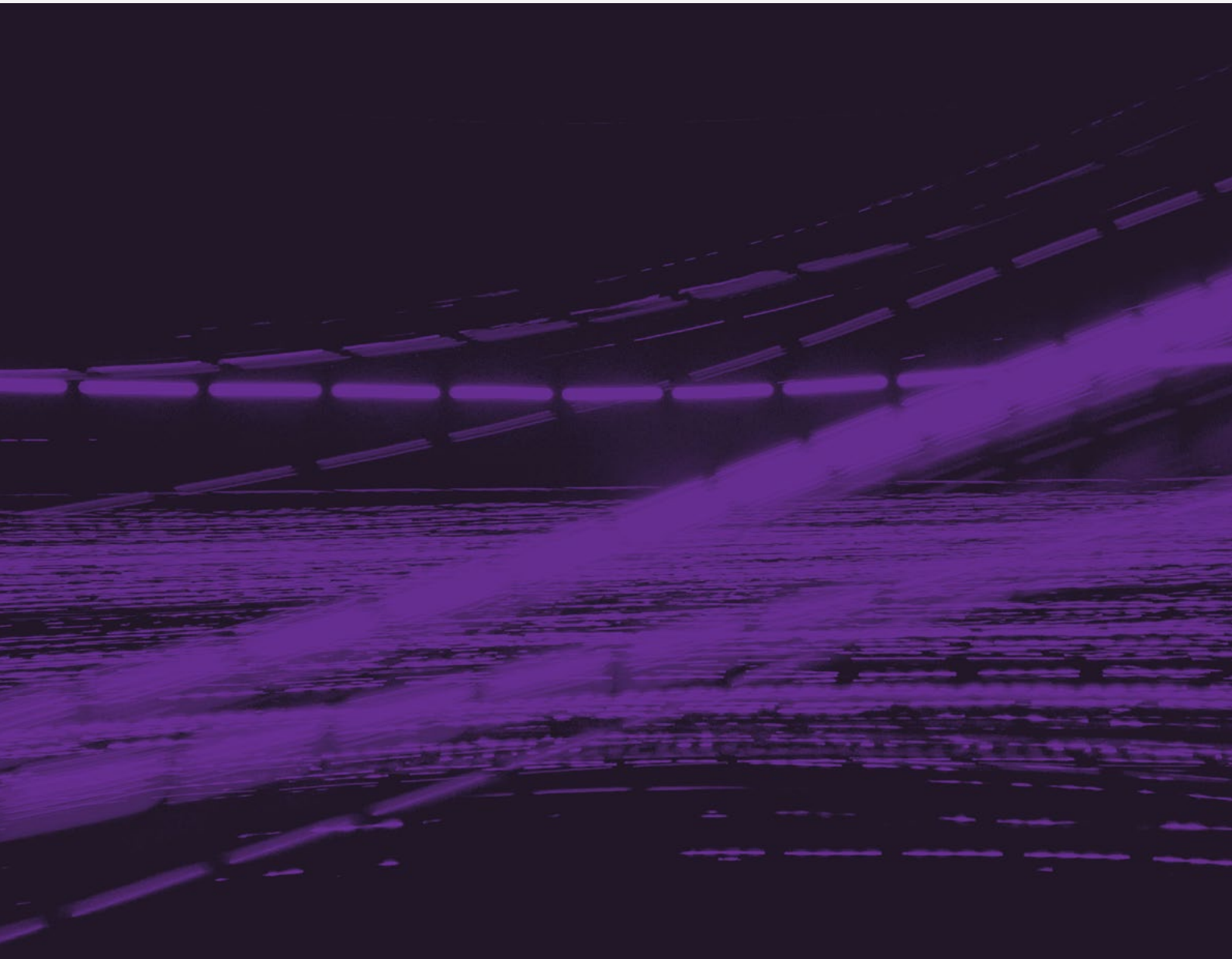
Direct attacks target either the user or administrator directly. One of the most popular methods in use at the moment is credential stuffing.

This is where hackers use stolen data (stolen username and password pairs) in combination on website log-in forms to try and find matches.

Since many users will re-use the same password and username/email, when those credentials are exposed (by a database breach or phishing attack, for example) submitting those sets of stolen credentials into dozens or hundreds of other sites can allow an attacker to compromise those accounts too.

To protect your website from hackers, there are simple steps you can take:

1. Install a strong firewall that can identify malicious requests and IP addresses;
2. Use a password manager to create strong, complex passwords that cannot be easily detected by an outside party;
3. Regularly update your software to ensure there are no vulnerabilities;
4. A Secure Sockets Layer SSL certificate will encrypt communication to and from your site and will prevent hackers from harvesting shared information;
5. Choose credible, well-reviewed plug-ins that update regularly and have been developed by a trusted source;
6. Put in place a dedicated website bot detection & prevent platform.



Veracity Trust Network

04
The Business Impact

Attackers are constantly crawling and snooping around websites to identify vulnerabilities to infiltrate websites.

The majority of motives driving cyberattacks are financial in motivation, but the methods in which they take place vary.

Stealing Data

Hackers are looking for access to sensitive user data including account details and passwords and they access it through phishing and social engineering attacks in the main, alongside malware and brute force attacks.

Using the stolen data, they can leave customers vulnerable to financial fraud and identity theft by impersonating them to transfer money from bank accounts, apply for loans, file for benefits etc.

Selling Data

Data is big money on the dark web. Cybercriminals purchase stolen data to orchestrate scams, financial fraud, identity theft, and to issue ransomware demands to companies who've had data stolen.

SEO Spam

Spamdexing, or SEO Spam, is used by hackers to reduce the ranking of a website and reroute legitimate visitors to spam websites and is a highly profitable scheme. They occur when hackers create backlinks and spam into user input fields on a business website.

By redirecting users to spam websites, they can steal data, gain access to credit card information and syphon money to illegitimate purchases of non-existent goods.

Malware

Hackers use websites to spread malware, including spyware and ransomware, to visitors who unknowingly will then pick up a bug which they distribute through their own systems to other websites and users.

This could be because they're doing it for their own benefit (blackmailing companies to pay a ransom to "free" their websites, selling data or stealing patented information, or they're employed by cybercriminals, competitors or, occasionally, nation-states, to cause disruption. This is another highly profitable type of hack.

Economic Consequences of Bot Attacks

Bot Attacks cost money.

The global average cost of a data breach in 2023 was $4.45m, a 15% increase over three years according to IBM.

In fact, according to Statista, the cost is predicted to reach $12.43 trillion by 2027, compared to $0.7trillion in 2017.

Global online fraud losses linked to bot attacks are projected to exceed $48 billion a year by 2023, and online fraud associated with bots is projected to grow 131.2% between 2022 and 2027, according to a report by Juniper Research.

And, according to UK Finance, which represents more than 300 firms across the industry, more than £1.2

billion was stolen by criminals through authorised and unauthorised fraud in 2022, equivalent to over £2,300 every minute.

Almost 80% of APP fraud cases start online (78%) and 18% starts via telecommunications scams. On top of this, positive action within the banking and finance industry prevented a further £1.2b of unauthorised fraud from getting into the hands of criminals.

Reputational Damage and Customer Trust

Of course, there is more than just a financial implication from suffering a bot attack.

Malicious bots mask themselves and are becoming cleverer, attempting to interact with applications or websites in the same way a legitimate human user would, this makes them much harder to detect and block.

Brand reputation and customer trust are immeasurably damaged and nearly half of consumers surveyed by IBM in its 17th Cost of a Data Breach Report said they would stop doing business with a company known to have experienced data breaches.

The IBM report also found 83% of studied organisations had experienced more than one data breach in their lifetime and, also of concern, nearly 50% of breach costs are incurred **more than a year** after the incident took place.

Cyberattacks could make your business uninsurable

According to Mario Greco, the head of one of Europe's biggest insurance companies Zurich, the rise in cyber-attacks could result in them being uninsurable.

He told the Financial Times that cyber-attacks, rather than natural disasters, would become uninsurable if the disruption from hacks continues to rise.

Zurich reached a settlement with multinational food and beverage company Mondelez International to close a $100 million lawsuit against the insurer for refusing to pay out on cyber claims related to the 2017 NotPetya attack.

In September 2022, Lloyd's of London defended a move to limit systemic risk from cyber attacks by requesting that insurance policies written in the market have an exemption for state-backed attacks.

From March 2023, all standalone cyber insurance policies underwritten by members of the sprawling Lloyd's of London marketplace *"must exclude liability for losses arising from any state-backed cyber-attack" the 300-year-old organisation warned – telling members that cyber-attack coverage "if not managed properly… has the potential to expose the market to systemic risks that syndicates could struggle to manage."*

Bots cause misinformation

Misinformation is another one of the many ways bots cause issues worldwide and, while you may think your brand is safe from that type of attack, the technology used to create bots which spread false data can also be used to cripple legitimate businesses.

Sites that depend on advertising or sell merchandise and only have limited stock availability are more vulnerable to bot traffic issues than some other business types.

Fake ad clicks for websites that depend on ad revenue can result in loss of earnings and damage to the company reputation because of action taken by advertising networks including removing the brand's ability to use them.

For eCommerce sites that have limited inventory, or which sell high value goods, scalpers have often used bots to snap up things like gaming consoles or event tickets. In other instances, bot owners have used them to dump inventory into thousands of carts, making items unavailable for genuine buyers.

Legal and Compliance Risks

The penalties for failing to protect against malicious bots can be severe, and understanding your legal and compliance risks is vitally important.

A breach of the EU's GDPR (General Data Protection Regulation), which the UK is still bound to, and which also applies to any organisation doing business within the EU, can be up to 20 million Euros, or up to 4% of the total global turnover of the previous year, whichever is higher.

The UK's Information Commissioner's Office (ICO) regularly publishes information about cyber and data breaches and the action it's taken, as well as guidelines for compliance and data processing, on its website.

It has created a number of resources for organisations and individuals about data protection and responsibilities.

The ICO is responsible for monitoring and enforcing a number of different Acts of Parliament and Regulations including: Data Protection Act, Freedom of Information Act, Privacy and Electronic Communications Regulations, General Data Protection Regulation, Environmental Information Regulations, INSPIRE Regulations, eIDAS Regulation, Re-use of Public Sector Information Regulations, NIS Regulations, and the Investigatory Powers Act.

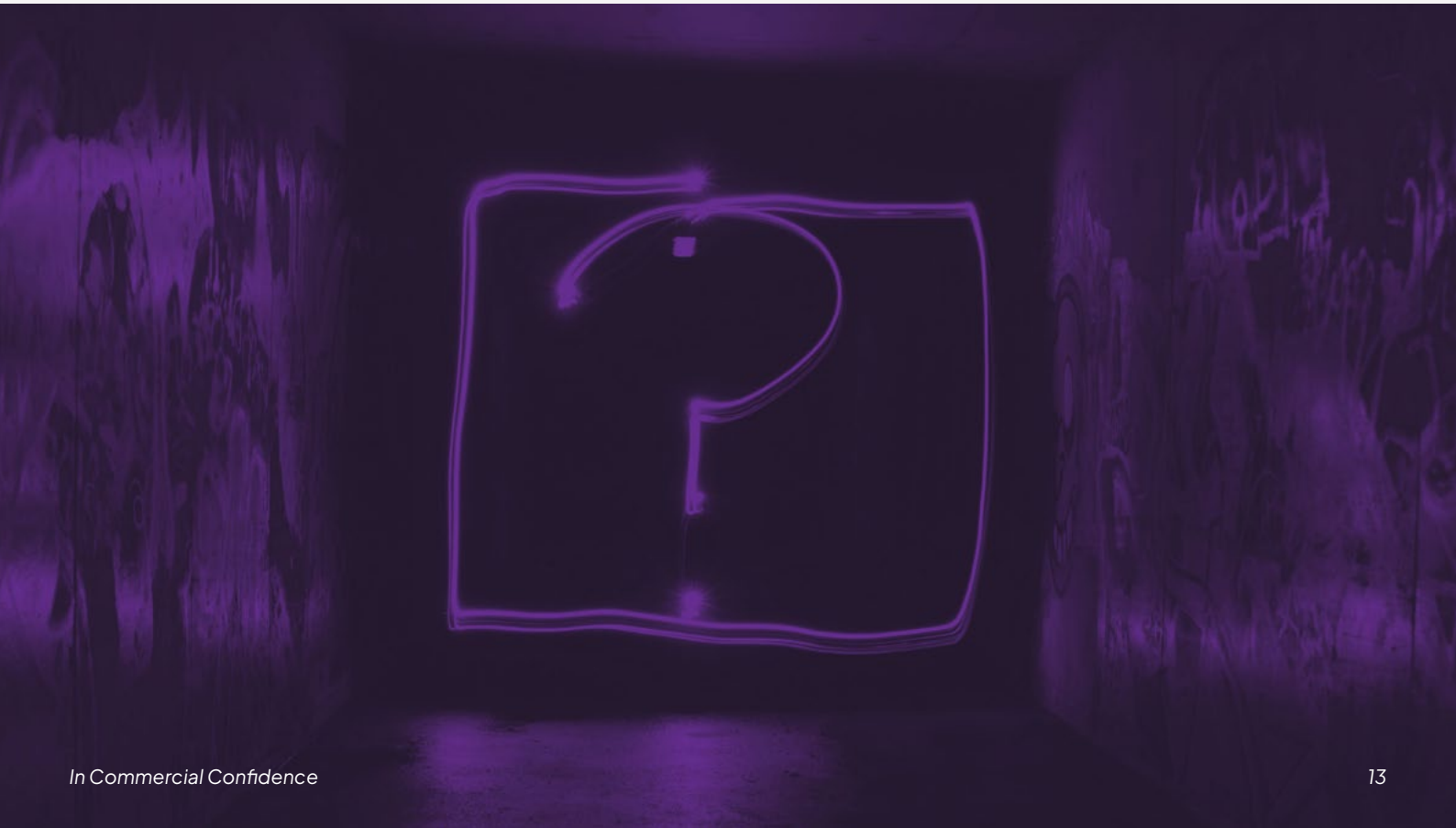
During 2022/23, the ICO handled almost 35,000 data protection complaints, working with organisations to make changes and encourage public trust and confidence. In April 2023 the ICO fined social media app TikTok £12.7 million for misusing children's data.

It also recently issued guidelines for website designers and developers, as well as businesses commissioning others to create their websites, for what it refers to as "damaging website design practices that may harm your users".

Ensuring that people can make effective, informed decisions is good both for competition and for privacy.

Used responsibly, online choices can be designed to empower users to make effective and informed choices about the way their personal information is used in digital markets, building customer trust.

Good design practice also helps reduce the risk factors for malicious bots being able to gain entry into your backend systems through website vulnerabilities.



Veracity Trust Network

05
Bot Identification and Prevention

When evaluating the traffic of your website, you can often glean summary information about potential bot activity just by analysing basic site metrics.

Collect Data

Making sure you're monitoring and reviewing in-depth analytics and other request data means you should be able to identify the holes in bots' disguises. Once you can separate human traffic from bot traffic, you can then dig deeper to identify the purpose of the bots.

Good bots including search engine crawlers from Google, Bing, Facebook etc, can be given access to your website.

Malicious bots can be isolated and blocked.

Evaluate Traffic

Bot traffic can be associated with high bounce rates or low conversion rates. Another strong indication of bots is unexplained traffic spikes or high requests to a particular URL.

On login pages, define your failed login attempt baseline, then monitor for anomalies or spikes. Set up alerts so you're automatically notified if any occur.

Identifying Risks

Stopping bot traffic begins with identifying potential risks to your website marketing, and eCommerce campaigns bring more bots.

Improved understanding of the ways your site could become a target is key to a successful bot management strategy. Some website functionalities are highly exploitable by bad bots.

Adding login functionality creates the opportunity for credential stuffing and credential cracking attacks, having a checkout form increases the chances of credit card fraud (carding/card cracking). Providing gift card functionality invites bots to commit fraud.

Make sure your website has added security functionality and stricter rules for these pages.

The Role of AI in Detecting Bots

The role of Artificial Intelligence (AI) in cybersecurity is one which is becoming increasingly important as malicious bots get even more clever in the ways they mimic human behaviour.

Using AI as part of the detection process for malicious bots brings the potential for organisations to spot bot-driven cyber-attacks more efficiently and also help them identify dangerous content that could potentially be missed otherwise.

According to the IBM Cost of Data Breaches survey, security AI and automation were shown to be important investments for reducing costs and minimizing time to identify and contain breaches.

Organisations that used these capabilities extensively within their approach experienced, on average, a 108–day shorter time to identify and contain a breach. They also reported $1.76 million lower data breach costs compared to organisations that didn't use security AI and automation capabilities.

Machine Learning (ML) and AI can help organisations

better recognise threats, respond to them, and stay one step ahead of hackers.

By merging various forms of data from anti-malware components on the host, network, and cloud, ML techniques can be utilised to enhance malware detection.

The key to all ML is a process called training, where a computer program is given a large amount of data - sometimes with labels explaining what the data is - and a set of instructions.

The program will then search for patterns in the data it has been given to achieve these goals.

Using AI in cybersecurity brings a lot of benefits to the table, including:

AI learns over time

AI uses ML and deep learning to recognise patterns and cluster them over time. These patterns help in securing security in the future. Since AI is always learning, it makes it very difficult for hackers to beat their intelligence.

AI can handle a lot of data

A company's network handles terabytes of data in a day. Protecting it from malicious people and software is not easy to do manually. AI provides the best solution to skim through massive data and incoming traffic chunks.

Improved detection and response times

Detecting a threat timely always saves you from irreversible damage to your network. AI ensures quick and effective scanning and response to any possible threats.

Better overall security

Combining all these advantages and possible applications in our daily life shows how effective the use of AI in cybersecurity will be. It will save time, and money and, above all, protect your networks from human errors.

Understanding Behavioural Analysis

AI can also be used alongside Machine Learning (ML) to understand behaviour both of genuine human visitors and malicious bots.

Building predictive models through the use of big data analytics has already helped the cyber security industry warn businesses about potential point of entry for cyber-attacks. AI and ML are key components in creating the algorithms necessary to gather and collate this big data.

One other tactic which is growing in popularity, is the use of a *"zero trust"* philosophy. This starts with the idea that every bot is treated as *"guilty until proven innocent"* and therefore interrogation and detection capabilities are deployed from the start of any request.

One a bot's status has been classified as either good or malicious, the software will then determine how it wants to manage it. Organisations can set their own parameters to ensure only wanted bots make it through to their website.

Identifying Advanced Bots: The Need for Real-Time Solutions

Part of the reason sophisticated bot attacks can be hard to stop is due to the complexity inherent in intelligent bots.

Internal fraud and security teams need to meticulously analyse signals and traffic patterns to suss out bots from real human users. Many modern intelligent bots have three times as many signatures than previous "dumb" bots, leading to an increase in the time fraud and security teams have to take in analysing the data, making accurate risk detection more difficult.

According to an article in Forbes, reactive fraud solutions that rely only on known patterns and historical data are fairly ineffective, because fraudsters use AI to evade detection and present signals meant to deceive most bot detection systems.

Ransomware is a major threat

A white paper from the NCSC and the National Crime Agency (NCA) said Ransomware had been the biggest development in cybercrime since it published the 2017 report on online criminal activity.

Ransomware is malicious software that prevents you from accessing your computer, or the data stored on it and demands ransom payment in order to regain access.

You can reduce the likelihood of malicious content reaching your devices through a combination of:

1. Filtering to only allow file types you would expect to receive;
2. Blocking websites that are known to be malicious;
3. Actively inspecting content;
4. Using signatures to block known malicious code.

Ransomware purveyors - who leverage malware to hold a company's computer systems or sensitive data hostage until a payment is made - have extorted a total of at least $449.1 million through June, according to Chainalysis.

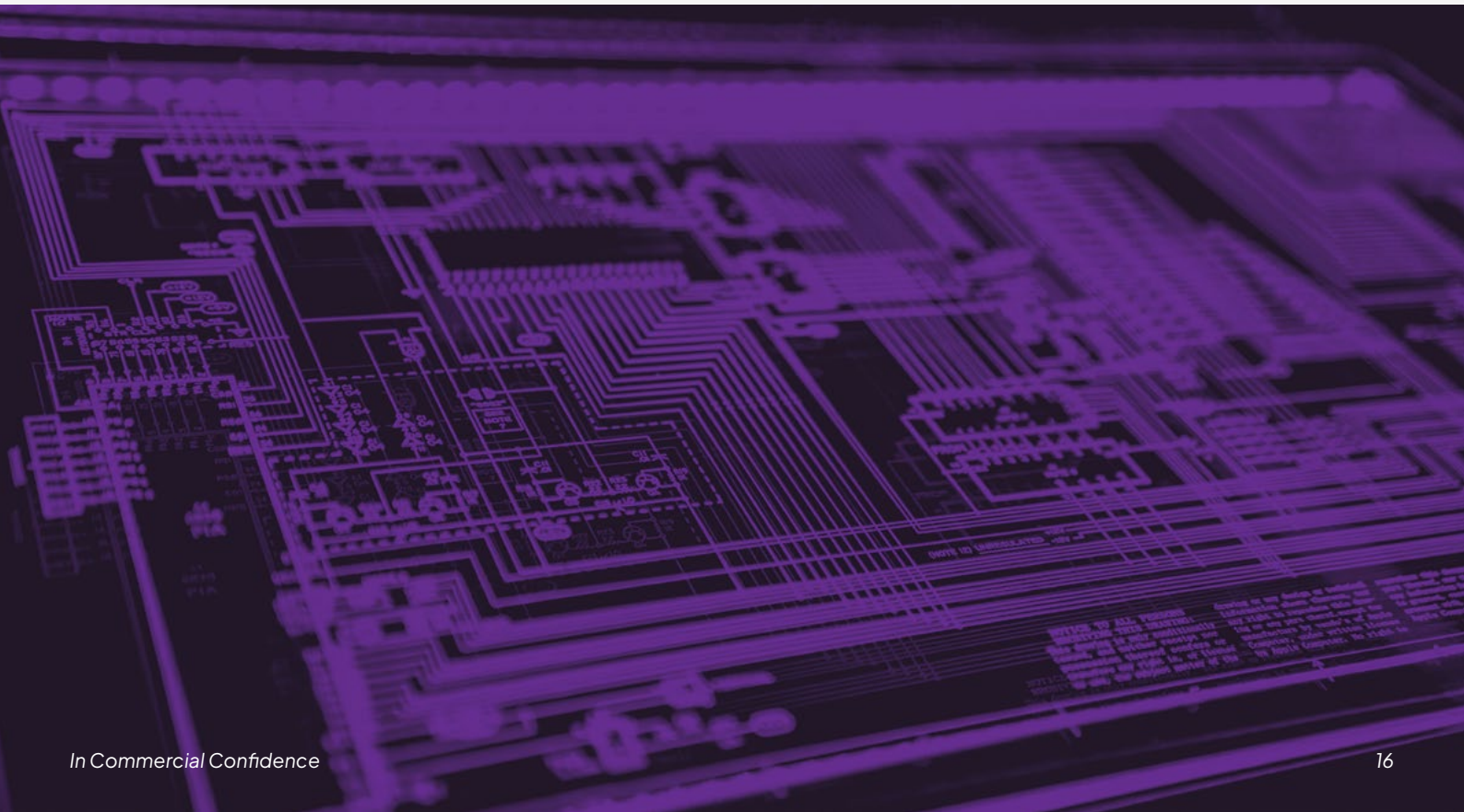
"Should this pace continue, the total yearly figure could reach nearly $900 million," a report from cyber risk management company Resilience said. *"This projection puts 2023 on pace to become the most financially damaging year for ransomware since 2021."*

The report adds that, when Resilience's claims data is overlapped with data from ransomware incident response partner Coveware, blockchain analytics firm Chainalysis, security partner Zscaler, and security firm Sophos, it reveals five key findings that impact both network defenders and the cyber insurance industry at large:

1. Enterprises are getting better at fighting ransomware extortions;
2. Return of Big Game Hunting;
3. Third-Party Vendors Take Over as Lead Point-of-Failure;
4. Cause-of-Loss Shifts from Ransomware to Encryption-less Extortion;
5. Cyber Crime is Indiscriminate.

As companies become more resistant to paying extortions, Resilience is seeing a move towards going after bigger fish and swimming upstream to hit vendors and bypass security controls.

This has significant implications for those defending their organisations and trying to limit financial losses from these actors.



Veracity Trust Network

06
Veracity Advanced Web Threat Protection

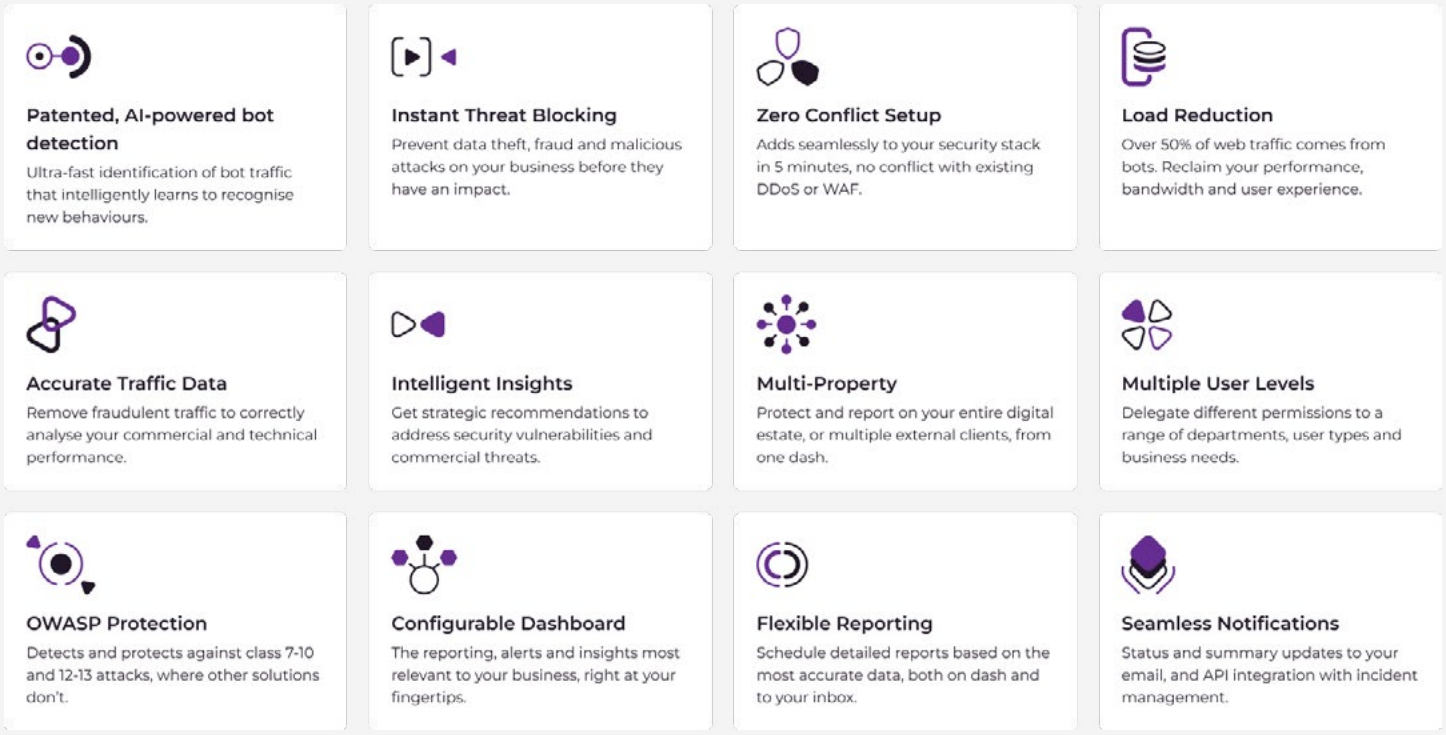
Having successfully created its award-winning Ad Fraud Protection platform, Veracity Trust Network unveiled the launch of its new Web Threat Protection Platform in March 2023.

This award-winning platform utilises ML to detect bots and safeguard online revenue, as well as providing a competitive edge and helping to protect brand reputation.

Veracity Web Threat Protection works effortlessly alongside your existing security stack and provides deep reporting insight into your system's true performance.

No more hunches, just transparent, real data. Veracity Web Threat Protection keeps your business safe, reduces wasted spend, improves customer experiences and gives you accurate information to grow.

Veracity Threat Protection stacks seamlessly with your DDoS and WAF solutions. This is because it's an essential, specialised answer to malicious bot activity. Not an add-on. Not an afterthought.



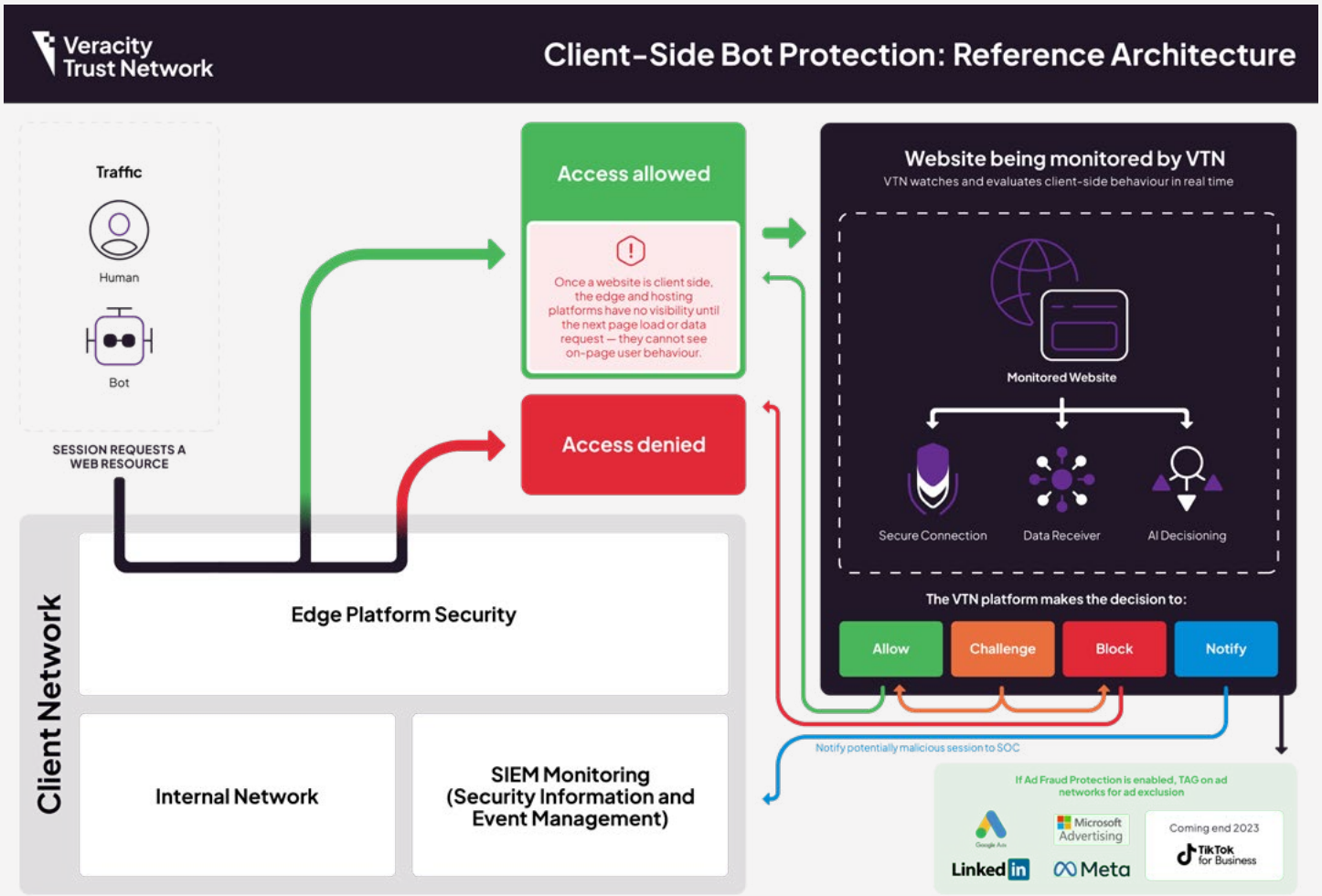
Proactive Bot Detection and Leveraging AI for Comprehensive Bot Defence

Our patented, AI-powered technology detects Automated Bot Attacks and Supply Chain Attacks (OWASP class 7–10 and 12–13) accurately, quickly and before they can cause you damage.

Evaluating and Implementing Veracity Advanced Bot Protection

Veracity enables organisations to gain visibility and control over human, good bot, and bad bot traffic without imposing friction on legitimate users; stopping 'bad bots' before they can do damage.

The Veracity platform complements existing cyber defences and is applicable to any organisation in regulated markets (such as financial services, where the consequence of data breach is severe) or businesses relying on website visitors for their success (such as eCommerce or online gaming, where it's vital to know the visitor is human).



Why We Are Different

Our technology began life as a tool to intelligently detect click fraud and save money for businesses using online advertising.

Once it became clear that our AI-powered detection engine could do even more, and protect people from legitimately dangerous bot attacks and compromised data, we developed Veracity Web Threat Protection.

Founded in 2016, Veracity was formed with one intention: to fight the rise of malicious bot activity.

To combat an ever-evolving threat, you need technology that's prepared for the unknowns just as much as the known predators. Our patented, AI-powered bot detection technology does just that.

Elegantly designed to mitigate everything from data theft attempts to advertising click fraud, our engine solves problems for multiple business functions. From security to finance, marketing to data analysis, customer experience and reputation management.

Why You Should Consider Us

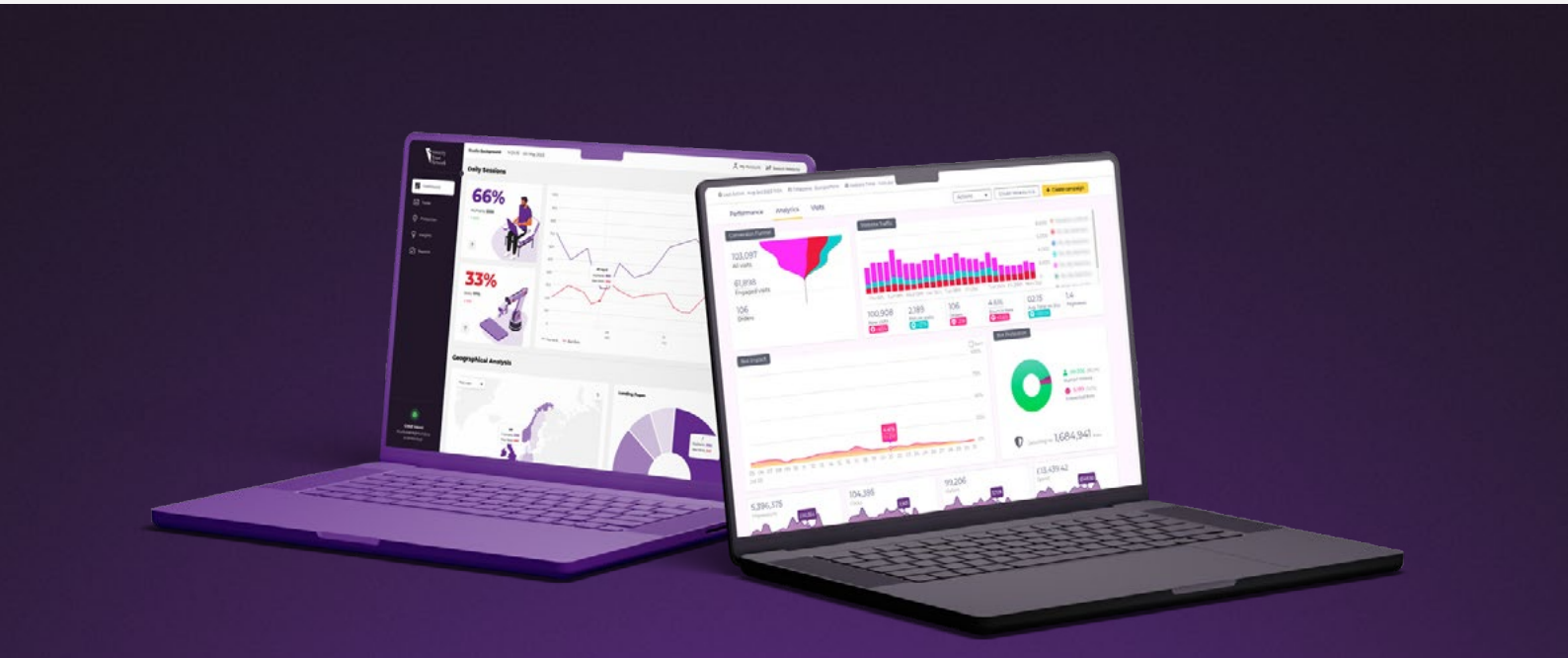
Veracity's Web Threat Protection is easy to install, within minutes you are protected and ready to go.

It is a point solution that works as a standalone or with other cyber solutions for a complete cyber defence. In addition, there are no subsequent operational overheads, no maintenance overheads and no third-party integrations required.

Web Threat Protection addresses all bot attack vectors (account takeover, fake account creation, data threat, ransomware etc) and has near 100% efficacy with false positive rates at or near zero (0.05%).

It includes uniquely patented AL MLM that works on both "proof of human" as well as "detection of bot" axes for greater effectiveness and includes a full monitoring dashboard that shows bot attack origins and where your potential vulnerabilities lie.

With full visitor journey and insight data based on humans-only data, for accurate web visit statistics, you can be assured the information you're receiving has been evaluated to give you valuable insights and guidance for action where you may need it.



Veracity Trust Network

07
The Roadmap Ahead

At the AI Safety Summit at Bletchley Park, the first held of its kind, 28 signatories agreed to the Bletchley Declaration.

Those represented were:

Australia, Brazil, Canada, Chile, China, the European Union, France, Germany, India, Indonesia, Ireland, Israel, Italy, Japan, Kenya, Kingdom of Saudi Arabia, the Netherlands, Nigeria, the Philippines, the Republic of Korea, Rwanda, Singapore, Spain, Switzerland, Türkiye, Ukraine, United Arab Emirates, the United Kingdom and the United States.

The agreement recognises a shared consensus on the opportunities and risks of AI, and the need for collaborative action on frontier AI safety.

The Bletchley Declaration, referring to the risks posed by the most advanced AI systems, states: ***"There is potential for serious, even catastrophic, harm, either deliberate or unintentional, stemming from the most significant capabilities of these AI models."***

Frontier AI refers to the most cutting-edge systems, which some experts believe could become more intelligent than people at a range of tasks.

Five objectives were identified during the summit which are covered by the declaration:

Objective 1

A shared understanding of the risks posed by frontier AI and the need for action.

Objective 2

A forward process for international collaboration on frontier AI safety, including how best to support national and international frameworks.

Objective 3

Appropriate measures which individual organisations should take to increase frontier AI safety.

Objective 4

Areas for potential collaboration on AI safety research, including evaluating model capabilities and the development of new standards to support governance.

Objective 5

Showcase how ensuring the safe development of AI will enable AI to be used for good globally.

The Bletchley Declaration also addresses future cooperation on AI research and development and notes in particular:

- Identifying AI safety risks of shared concern, building a shared scientific and evidence-based understanding of these risks, and sustaining that understanding as capabilities continue to increase, in the context of a wider global approach to understanding the impact of AI in our societies.
- Building respective risk-based policies across our countries to ensure safety in light of such risks, collaborating as appropriate while recognising our approaches may differ based on national circumstances and applicable legal frameworks. This includes, alongside increased transparency by private actors developing frontier AI capabilities, appropriate evaluation metrics, tools for safety testing, and developing relevant public sector capability and scientific research.

White House takes action

The White House stated in October that it had taken what it was calling ***"the most significant actions ever taken by any government to advance the field of AI safety,"*** when it announced an executive order from President Joe Biden.

The US measures include:

- Creating new safety and security standards for AI, including measures that require AI companies to share safety test results with the federal government;
- Protecting consumer privacy, by creating guidelines that agencies can use to evaluate privacy techniques used in AI;
- Helping to stop AI algorithms discriminate and creating best practices on the appropriate role of AI in the justice system;
- Creating a programme to evaluate potentially harmful AI-related healthcare practices and creating resources on how educators can responsibly use AI tools;
- Working with international partners to implement AI standards around the world.

UK Issues Warnings About Commercial Hacking Tools

A new report from the UK's National Cyber Security Centre (NCSC) has warned of the rising threat from irresponsible use of commercial hacking tools over the next five years.

Customisable tool frameworks are developed by cyber security software developers to emulate threat activity to enable penetration testing of networks. They are usually sold under licence, but some are also publicly available or available in versions where the licence has been removed.

It highlights how, over the past decade, more than 80 countries have purchased cyber intrusion software. While products vary in capability and application, commercially available spyware for mobile devices can offer the ability to read messages, listen to audio calls, obtain photos, locate the device and remotely operate the camera and microphone.

Emerging Bot Threats and Trends

The NCSC has also said there are growing cybersecurity risks of individuals manipulating prompts through *"prompt injection"* attacks on chatbots.

Chatbots are large language models (LLMs), such as OpenAI's ChatGPT and Google's AI chatbot Bard.

A *"prompt injection"* attack is where a user creates an input or a prompt that is designed to make a language model - the technology behind chatbots - behave in an unintended manner.

Because chatbots are used to pass data to third-party applications and services, NCSC believes that risks from malicious prompt injection will grow.

It also believes these types of attacks can also cause real-world consequences if systems are not designed with security. The vulnerability of chatbots and the ease with which prompts can be manipulated could cause attacks, scams and data theft.

AI-enabled interfaces could be used to:

- Use AI voice cloning for voice-based phishing (vishing) attacks to impersonate employees to gain privileged access;
- Tailor email-based phishing attacks with native language accuracy in multiple languages;
- Discover and identify zero-day vulnerabilities that can be leveraged for initial access;

- Reduce the time required to develop malicious code and lower the bar for entry.

This could lead to cybercriminals doubling down on ransomware as a means of generating revenue, rather than them abandoning it in favour of a new strategy.

Ransomware attacks increased by more than 37% in 2023 compared to the previous year according to Security Service Edge (SSE) experts Zscaler. The company also found the average enterprise ransom payment exceeded $100,000, with a $5.3m average demand.

PwC has identified two further emerging threats in ESG reporting fraud and supply chain fraud.

Although the figures for these are low at the moment, with only 8% of companies reporting fraud identifying experiencing ESG reporting fraud, and only 13% seeing new incidents of supply chain fraud, these are areas PwC predicts will become higher within the next couple of years.

The Future of Bot Defence

Organisations should be using advanced IP intelligence to identify proxies and employ a graduated approach to then taking action on these requests.

Robust analysis of user behaviour using both behavioural biometrics and behavioural analysis is also effective. These two systems examine the way in which a user interacts with a device and then analyses the actions to give context. Using these two systems together can help differentiate human from bot.

Broadly speaking, there are three goals a good bot detection software should meet:

1. Monitoring websites, networks, or applications;
2. Identifying bots or any malicious bot activity;
3. Preventing access or blocking actions performed by botnets.

In cybersecurity, many botnet detection strategies revolve around data packet analysis, which can identify irregularities in data transmission to a server.

In fraud prevention and detection, a combination of risk rules will help highlight suspicious bot activity, which can then automatically be blocked or reviewed.

Bot detection service vendors deliver techniques that vary, but there are a few recurring features:

- **IP lookup and analysis:** Understanding the type of online connection used by your website visitors can filter out bots and let through humans.
- **Device fingerprinting:** Analysing the combination of software and hardware used to connect to your site can point to suspicious activity – especially for botnets using the same devices or spoofing tools.
- **Velocity risk rules:** In bot detection, velocity rules allow you to learn how often someone does something online, providing insight into their behaviour and motivation. This helps you identify bots that perform the same action or sequences of actions repeatedly.
- **Real-time alerts:** You may have to deal with spikes in traffic that could point to a botnet attack. It's important to safeguard your website by creating fraud alerts for that purpose.

Veracity Trust Network

08 Conclusion

The world is in the middle of a technological revolution which is likely to bring with it developments which dwarf those of the industrial revolution of the 1800s.

AI and ML, along with other technologies, are fundamentally changing the way we live, work and relate to each other. AI is already transforming many industries and it promises to bring further developments for almost every aspect of both our economy and our society.

This brings huge opportunities, but also risks that have the potential to threaten not only organisations at a simple level, but globally at national level.

Businesses must take cybersecurity seriously and look at how their operations are protected from malicious bots taking over their websites and also seeking to compromise their data and hold it for ransom.

There are currently no standards for AI adoption, which means even legitimate uses can be compromised by agents with malicious intent. Website vulnerabilities are changing at a rapid pace, old technology which used to keep out non-human traffic, like CAPTCHA, is now vulnerable to sophisticated human-like bots which can mimic behaviour to a degree which is difficult to identify.

Web Threat Protection platforms like Veracity help provide a front line of defence against this increasingly intelligent malicious technology. AI and ML works at the core of the platform to identify and mitigate against changing threats. The technology identifies human like behaviour from malicious bots, that edge platforms miss.

With more than 50% of web traffic being bot traffic, and malicious, illegal bot attacks on the rise, it's your business's security, reputation and data compliance, that's on the line.

The Urgent Need to Address Bot Threats

A cybercriminal needs two things to make bot-related cybercrime a success – a valuable demographic and the technology to go undetected by their victims.

Currently the rapidly changing technology being used to create malicious bots means it's almost impossible to completely protect your organisation against them.

To mitigate this situation, you should be adopting a "*defence-in-depth*" approach starting from your website and using different layers of defence with mitigations in each level.

This will provide more opportunities to detect malicious bots and traffic and stop it before it causes real harm. Take steps to limit the impact malware could have on your business by assuming you will become a victim to it at some point.

There are actions you can take in preparation which will help defend against malicious bots.

Make Regular Backups

Make regular backups of your most important files - it will be different for every organisation - check that

you know how to restore files from the backup, and regularly test that it is working as expected.

Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment.

Make sure that the devices containing your backup (such as external hard drives and USB sticks) are not permanently connected to your network. Attackers will target connected backup devices and solutions to make recovery more difficult.

Prevent malware spreading

Prevent malware spreading across your organisation by following NCSC guidance on preventing lateral movement.

You can reduce the likelihood of malicious content reaching your devices through a combination of:

- Filtering to only allow file types you would expect to receive;
- Blocking websites that are known to be malicious;
- Actively inspecting content;
- Using signatures to block known malicious code.

Patch known vulnerabilities in all remote access and external facing devices immediately and follow vendor remediation guidance including the installation of new patches as soon as they become available. This applies equally to website plugins and code updates for services on hosted sites like WordPress or Wix.

Evaluate website traffic

When evaluating the traffic of your website, you can often glean summary information about potential bot activity just by analysing basic site metrics.

Key metrics to look for that could indicate you're being attacked by bots include:

- Average session duration: when the average session length is just a few seconds.
- Geo-location: when the geo-location of the traffic is either non-discernible or from all over the world.
- Traffic source: when the traffic source is mostly direct for that particular day and it usually isn't.
- Bounce rate: when the bounce rate is more than 95%.
- Service provider: when the majority of the traffic is from the same service provider.

Plan for an attack

Even if you think it's unlikely you'll be a victim of cybercrime, you should plan for an attack. Many businesses have found themselves being impacted by attacks further up a supply chain even if they weren't the intended target.

Plan for an attack, even if you think it is unlikely. There are many examples of organisations that have been impacted by collateral malware, even though they were not the intended target.

Develop a strategy for dealing with an attack, including a communications plan so that the necessary stakeholders are informed. Identify your legal obligations regarding the reporting of incidents to regulators and how soon this must be done.

The NCSC's free Exercise in a Box online tool, contains materials for setting up, planning, delivery, and post-exercise activity.

Veracity Trust Network

Get in Touch

Discover the Scale of Malicious Bots on Your Website

Book your Veracity 14-day Threat Assessment Today

Veracity Web Threat Protection is a powerful answer with an incredibly simple set up in minutes.

Either set and forget to block the bots with peace of mind or use its powerful intelligence tools to improve your performance, ROI and security.

Want to see how many bots have you in their sights right now?

Get started in minutes

veracitytrustnetwork.com
hello@vtn.live
UK +44 (0) 5603 861 037
US +1 (833) 286 6284

VeracityTrust
veracitytrustnetwork

Sources

https://www.csoonline.com/article/567775/uk-cybersecurity-statistics-you-need-to-know.html
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258
https://www.forbes.com/sites/forbestechcouncil/2022/11/18/the-intelligent-bot-revolution-what-businesses-need-to-know/?sh=454370776b1d
https://www.techradar.com/news/heres-how-to-spot-a-bot
https://www.verizon.com/business/resources/T218/reports/2023-data-breach-investigations-report-dbir.pdf
https://uktechnews.co.uk/2023/10/18/threat-spotlight-how-bad-bot-traffic-is-changing/
https://seon.io/resources/guide-to-bot-mitigation/
https://www.ncsc.gov.uk/collection/small-business-guide
https://www.ncsc.gov.uk/ransomware/home
https://www.nationalcrimeagency.gov.uk/news/all-news?searchword=&searchphrase=all&limit=5&areas[0]=news&news_topics[0]=cyber-crime
https://www.nationalcrimeagency.gov.uk/nsa-cyber-crime
https://www.ncsc.gov.uk/information/how-cyber-attacks-work
https://www.nationalcrimeagency.gov.uk/nsa
https://www.cloudflare.com/en-gb/learning/bots/what-is-a-bot-attack/
https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-uk-tr-state-of-the-phish-2023.pdf
https://www.bbc.co.uk/news/topics/c1xp19421ezt
https://www.bbc.co.uk/news/business-67149919
https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app
https://www.bbc.co.uk/news/business-60478725
https://www.ncsc.gov.uk/news/festive-shoppers-urged-to-be-cyber-aware
https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/stepping-ahead-of-risk-trend-micro-2023-midyear-cybersecurity-threat-report
https://www.dentons.com/en/insights/articles/2022/july/21/the-regulatory-landscape-surrounding-the-use-of-bot-technologies
https://www.oreilly.com/content/an-overview-of-the-bot-landscape/
https://medium.com/@hive42designs/bots-in-the-shadows-the-untold-story-of-internet-automation-and-its-consequences-695fe27d44af
https://www.secureworld.io/industry-news/bad-bots-unleashing-havoc
https://www.tryswivl.com/blog/how-ai-bots-are-changing-digital-marketing
https://standict.eu/news/trusted-information-digital-space
https://www.cloudflare.com/en-gb/lp/ppc/bot-management/
https://usercentrics.com/data-privacy-audit/
https://www.hackerone.com/reports/rethink-traditional-pentests
https://www.akamai.com/solutions/security/app-and-api-security
https://transparencyreport.google.com/safe-browsing/search?hl=en
https://www.getsafeonline.org/
https://www.ncsc.gov.uk/cyberaware/home
https://www.ncsc.gov.uk/
https://www.nationalcrimeagency.gov.uk/
https://rockcontent.com/blog/how-to-check-if-a-website-is-secure/
https://it.wisc.edu/news/two-things-to-look-for-in-a-secure-website/
https://support.google.com/chrome/answer/95617?hl=en-GB
https://guard.io/lp
https://www.bu.edu/tech/support/information-security/security-for-everyone/how-to-identify-and-protect-yourself-from-an-unsafe-website/
https://www.indusface.com/blog/what-is-a-website-vulnerability-and-how-can-it-be-exploited/
https://www.siteimprove.com/toolkit/accessibility-checker/
https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/
https://www.toptal.com/cyber-security/10-most-common-web-security-vulnerabilities
https://www.veracode.com/state-of-software-security-report
https://ca.godaddy.com/blog/how-hackers-can-tell-if-your-website-is-a-good-target/
https://vulcan.io/blog/owasp-top-10-vulnerabilities-2022-what-we-learned/
https://www.indusface.com/blog/how-do-websites-get-hacked/
https://datadome.co/bot-management-protection/good-bots-vs-bad-bots-and-when-you-should-block-them/