



## Malicious Bots:

Protecting your Digital Business from the Foot Soldiers of Modern Cyber Attacks



 **Veracity  
Trust Network**

<https://veracitytrustnetwork.com/>

## Structure of this presentation

1. Introduction
2. What is a bot?
3. Detecting bots is difficult.
4. Why do you need to care?
5. Sector case study – phishing in the legal sector.
6. Summary.

# Introduction



<https://veracitytrustnetwork.com/>

# Malicious Bots: Protecting your Digital Business from the Foot Soldiers of Modern Cyber Attacks

Stewart Boutcher, CTO Veracity Trust Network.

<https://www.linkedin.com/in/thebluehand/>



The image shows a LinkedIn profile card for Stewart Boutcher. At the top is a banner image of a city skyline. On the left is a circular profile picture of Stewart wearing sunglasses. To the right of the profile picture is a blue pencil icon. Below the profile picture, the name "Stewart Boutcher" is displayed with a verified badge and "(He/Him)" in parentheses. The bio reads: "Tech & Data lover. Speaker on Cybersecurity, AI, Quantum. Finalist 2023: Global Tech Entrepreneur + UK Tech Leader of the Year. DMA Council Member. Rock climber + whippet owner." Below the bio is the location "Greater Leeds Area" and a link for "Contact info". To the right of the bio are two organization logos: "Veracity Trust Network" and "Aberystwyth University".



<https://www.linkedin.com/in/thebluehand/>

Finalist 2023: Global Tech Entrepreneur + UK Tech Leader of the Year



# The Bot Defense Experts

## ABOUT US

Veracity Trust Network is a UK headquartered cybersecurity company.

We are active in the UK, ASEAN, Australia, the US and the GCC, with offices in the UK and Singapore.

We have clients in the legal sector, ecommerce, regulated industries and finance.

We have international patents and invest heavily in R&D.

## WHAT WE DO

Our focus is on detecting & preventing malicious bots on websites, progressive web apps and mobile apps.

Our 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.

We are always looking for ways to innovate and put our customers ahead of the bot makers.



# Malicious Bots: Protecting your Digital Business from the Foot Soldiers of Modern Cyber Attacks

















Stewart Boutcher, CTO Veracity Trust Network.

<https://www.linkedin.com/in/thebluehand/>

We are award-winning experts in protecting public facing platforms from bots.

We are proud alumni of the UK Government Cyber Runway 2023 Cohort, for leading UK cyber companies. Read more at [Cyber Runway Scale - Plexal](#)

We are global AWS Technology Partners.

			
Regional Winner Tech Nation Rising Stars Awards 2020	Best Martech Innovation - Won Prolific North Tech Awards 2021	Cyber Award Winner Tech Nation Rising Stars 3.0 Awards 2021	Best Marketing Tool - Won B2B Marketing Expo Innovation Awards 2021
			
Innovation of the Year - Won Digital City Award 2022	Innovation in Cyber Award - Finalist The National Cyber Awards 2022	Emerging Technology of the Year - Finalist UK IT Industry Awards 2022	Best Innovation - Won Best Business Awards 2022
			
Best Digital Tool or Software - Finalist Northern Digital Awards 2022	Tech Entrepreneur of the Year, Stewart Boutcher - Finalist Global Business Tech Awards 2023	AI-Enabled Data Solution of the Year - Finalist Data IQ Awards	Tech Innovation of the Year - Won Leeds Digital Festival Awards 2023
			
Cyber Security Company of the Year - Finalist UK Business Tech Awards 2023	Best Use of AI - Highly Commended Prolific North Tech Awards 2023		



Shortlisted as:  
UK's Most Innovate Cyber SME 2024



We are a corporate partner of the Association of Information Security Professionals (AiSP) in SE Asia



---

What is a bot?

## What is a bot?

A bot is a software application that is programmed to do certain tasks with a degree of automation & autonomy.

A malicious bot has been programmed to infect a system, steal data, or commit other criminal activities.



Feb 16, 2024 - Technology

# Department of Justice takes down Russian intelligence botnet



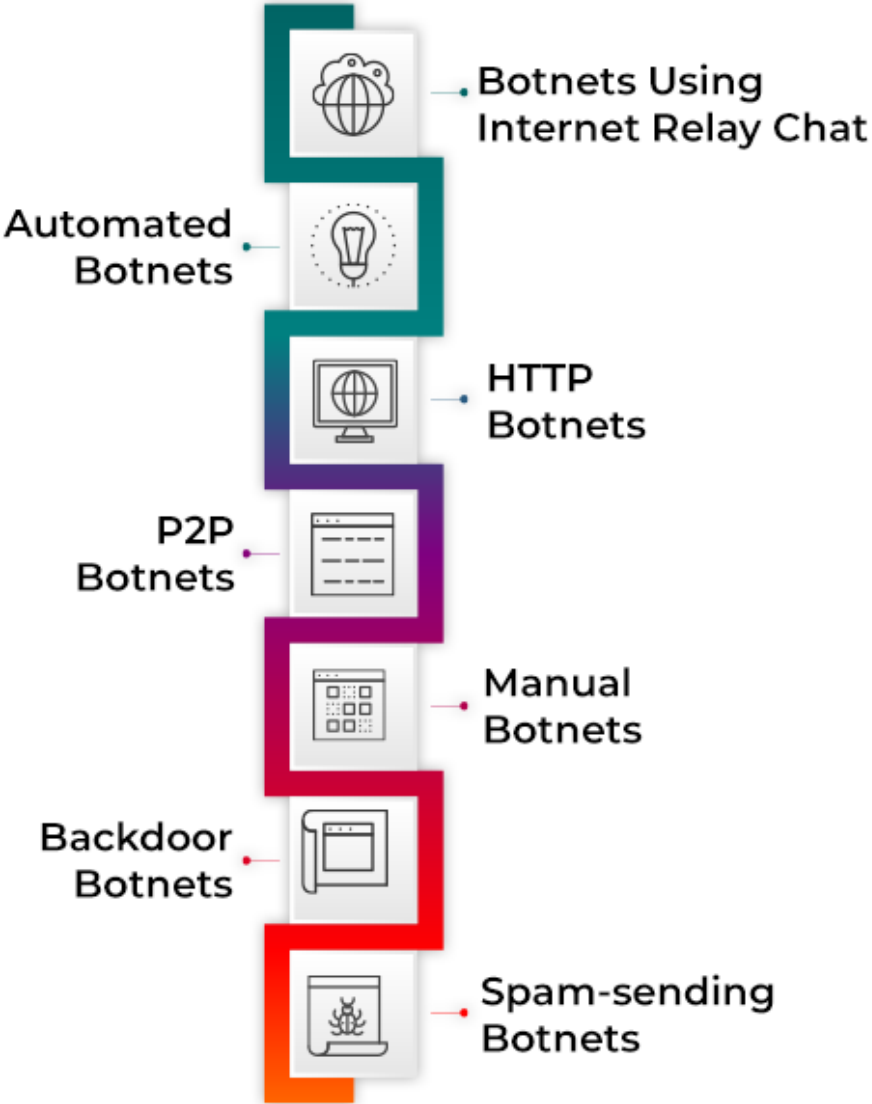
## What is a botnet?

Bots are generally run in collections known as “botnets” with some form of command-and-control structure.

Botnets may consist of bots on compromised PCs, cloud servers, mobile devices, “in-house” hardware, network devices, or more regularly a mix of all.



# TYPES OF BOTNETS

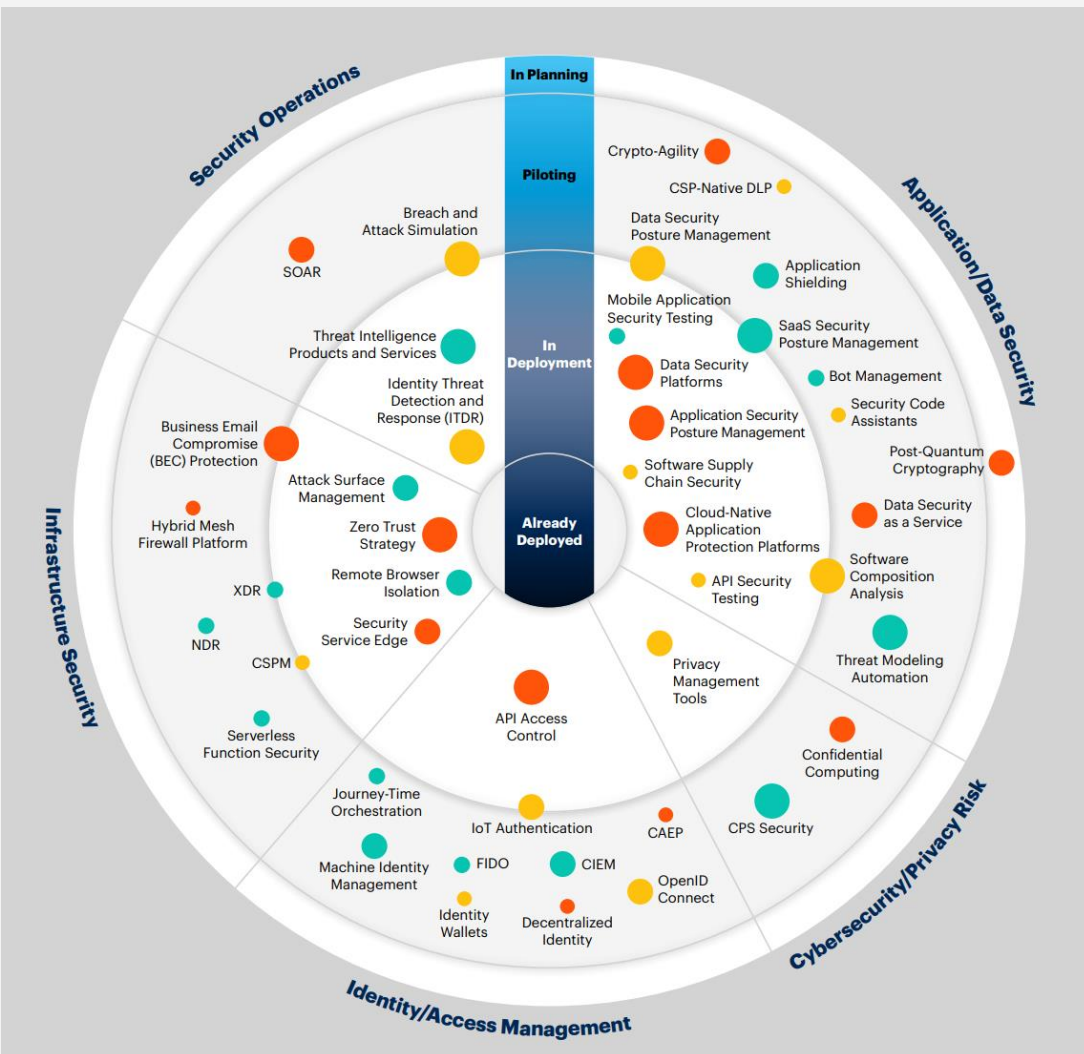


# The Dark Side Unleashed: The Threat of AI-Powered Botnets

“AI algorithms can optimise attack strategies by analysing network vulnerabilities, evading detection mechanisms, and exploiting weaknesses in real time...This enables them to develop new attack techniques at an alarming pace”



## Where bot protection fits into cybersecurity



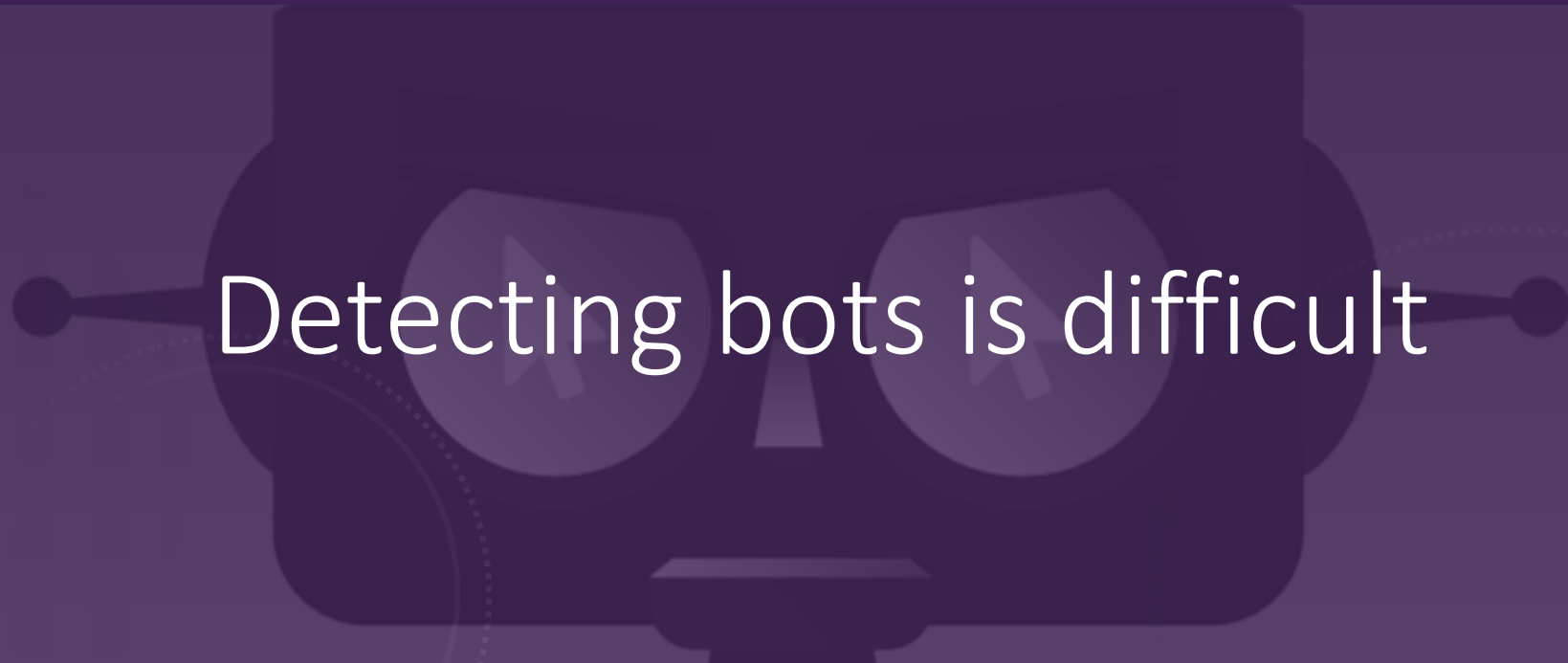
Gartner®

“2024 Technology Adoption Roadmap for Security and Risk Management”





Detecting bots is difficult



“



Detecting bots is difficult because the sophisticated ones try to appear human and evade detection. Your bot management solution must protect from every OWASP automated threat and be accurate in detecting the difference between human and bot traffic on your website, mobile apps, and APIs.

Open Web Application Security Project – [owasp.org](https://owasp.org)

“

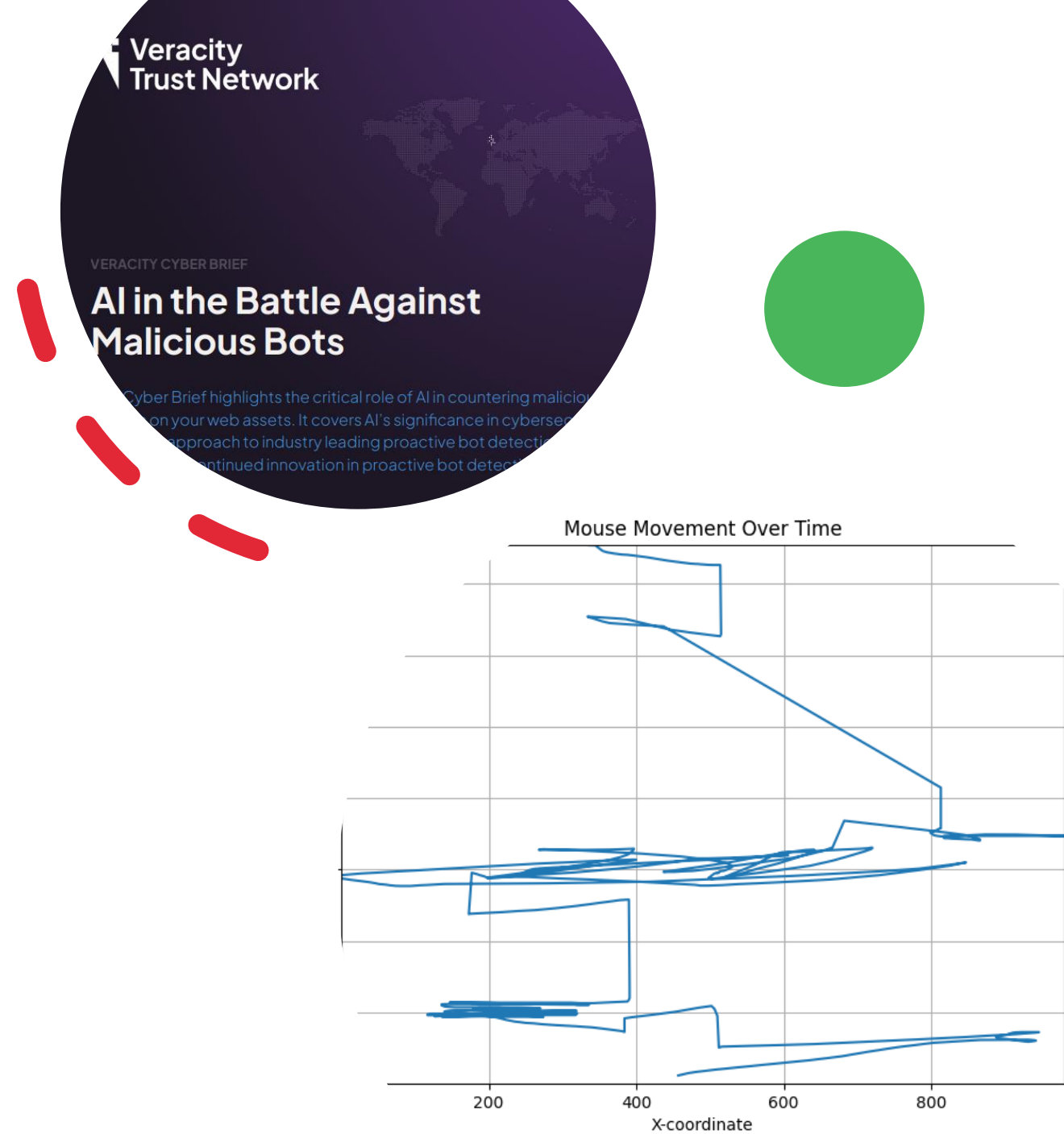
**Forbes**

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

The Intelligent Bot Revolution: What Businesses Need To Know



- At Veracity we understand the changing landscape of cybersecurity.
- We use supervised and unsupervised Machine Learning (ML) to look for indicators of bot behaviour and indicators of human behaviour.
- Allows for a network that analyses over 1,000 data features per journey.
- The result is a high-performance bot detection algorithm.
- ML algorithms can be retrained on new data to ensure stable high performance over time.

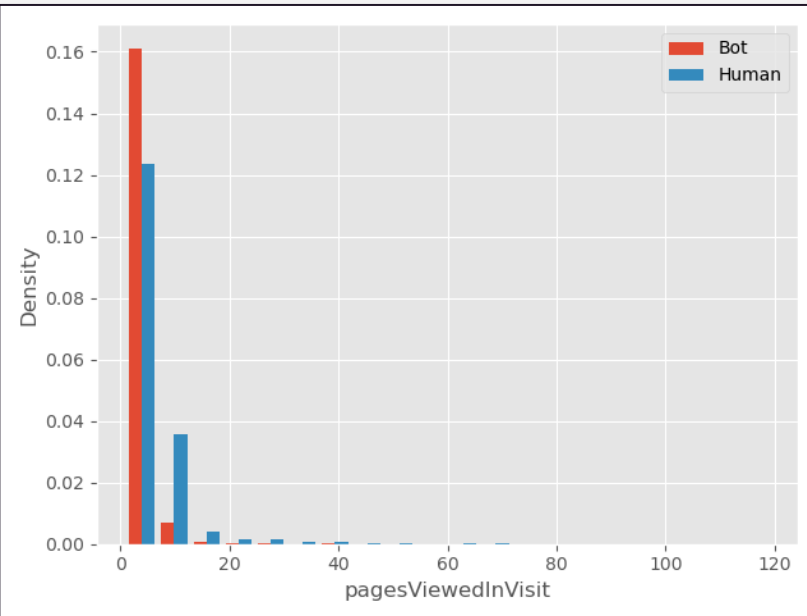




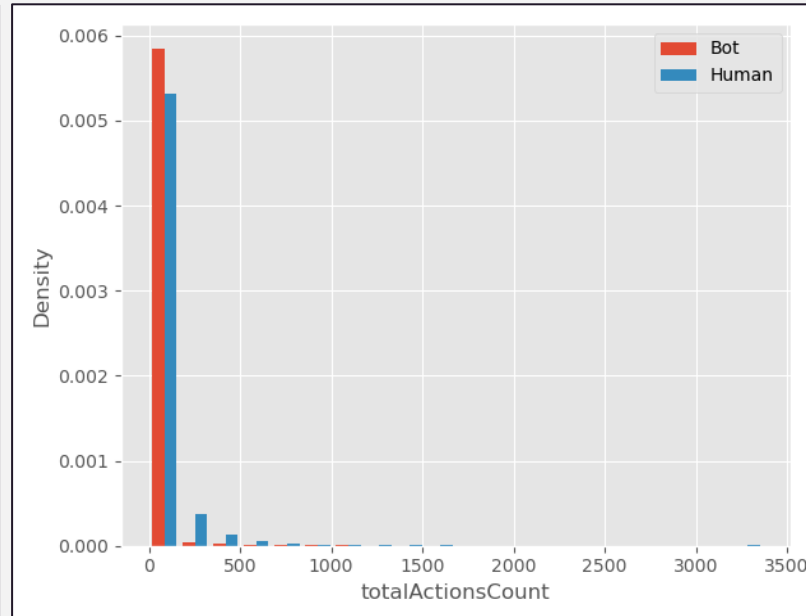
### Key Takeaways:

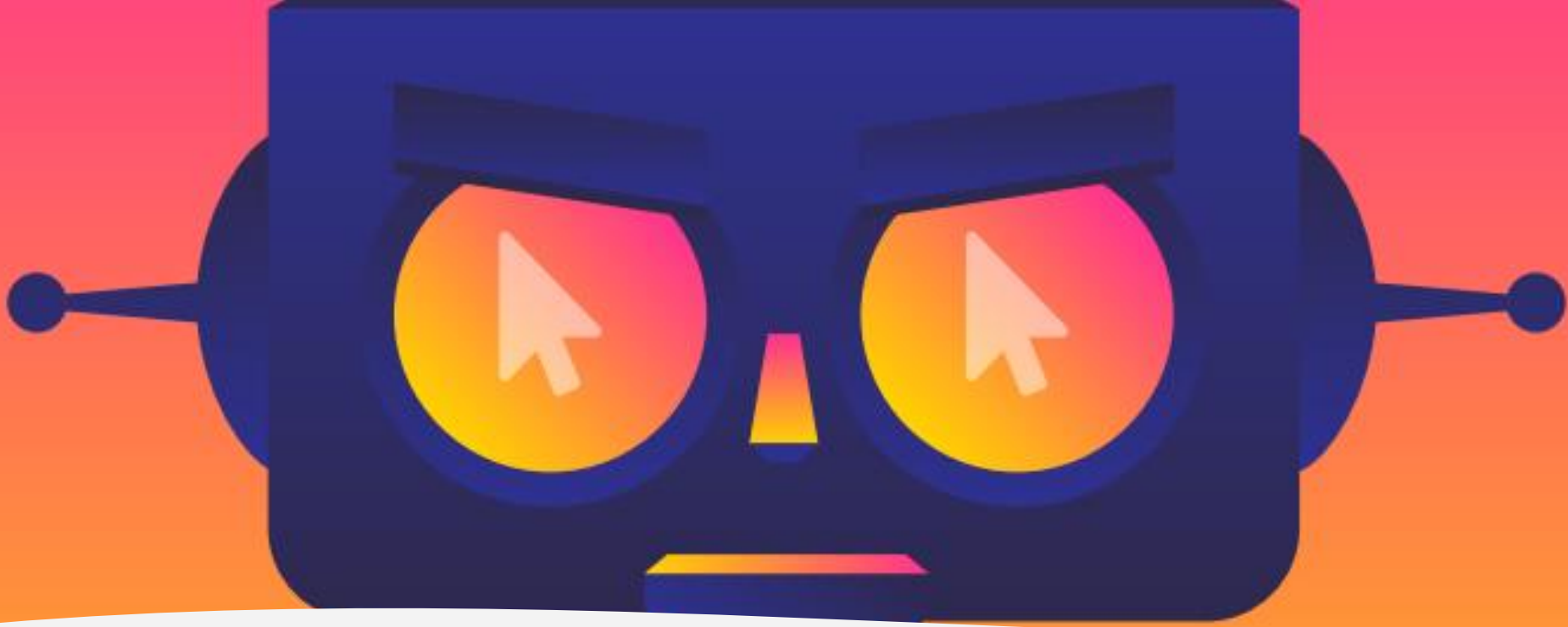
- Analysis shows that there are differences between human behaviour and most malicious bot behaviour
- A large amount of analysis was required to show a small number of these differences
- Increases in malicious bot sophistication means these differences will decrease over time
- Traditional, rules-based bot detection systems are becoming obsolete

## Examples of small differences



Comparison of Number of Pages Viewed in a Visit Between Bots and Humans





Why do you need to care?

# Malicious Bots: Protecting your Digital Business from the Foot Soldiers of Modern Cyber Attacks



Stewart Boutcher, CTO Veracity Trust Network.

<https://www.linkedin.com/in/thebluehand/>

Market Sector	Types of Businesses Included...	Damaging Bot Activity includes...
<b>Automotive</b>	Manufacturers, dealerships, vehicle marketplaces	Price Scraping, Data Scraping, Inventory Checking
<b>Business Services</b>	Real estate, CRM systems, business legal & financial services	Attacks on the API layer, Data Scraping, Account Takeover
<b>Education</b>	Online learning platforms, schools, colleges, universities	Account Takeover for students & course availability, scraping proprietary research papers and data
<b>Entertainment &amp; Arts</b>	Streaming services, ticketing platforms, production companies, venues	Account Takeover, Price Scraping, Inventory Checking, Scalping
<b>Financial Services</b>	Banking, Insurance, Investments, M&A, Cryptocurrency	Account Takeover, Card Cracking, Content Scraping
<b>Food &amp; Beverage</b>	Delivery services, online shopping, F&B brand sites	Credit Card Fraud, Gift Card Fraud, Account Takeover
<b>Gaming &amp; Gambling</b>	Online gaming, casinos, sports betting	Account Takeover, Odds Scraping, account creation for promotion abuse
<b>Government</b>	Government & agency websites, public services, local authorities	Account Takeover, Data Scraping of business & voter information
<b>Healthcare</b>	Health services, pharmacies	Account Takeover, Content Scraping, Inventory Checking, Vaccine appointments/availability
<b>Information Tech</b>	IT services, IT providers, services, technology providers	Account Takeover, Scraping
<b>Marketing</b>	Marketing Agencies, Advertising Agencies	Custom Content Scraping, ad fraud, denial of service
<b>News &amp; Media</b>	News sites, online magazines	Custom Content Scraping, ad fraud, comment spam, fake accounts
<b>Retail</b>	eCommerce, marketplaces	Denial of Inventory, Credit Card Fraud, Gift Card Fraud, Account Takeover, Data and Price Scraping
<b>Society</b>	Non-profits, faiths & beliefs, online dating, online communities	Data Scraping, Account Takeover, account creation, testing stolen card on donation pages
<b>Sports</b>	Updates, news, live score services	Data Scraping (live scores, odds, etc.)
<b>Telco</b>	Telco providers, ISPs, hosting providers	Account Takeover, competitive Price Scraping
<b>Travel</b>	Airlines, hotels, holiday booking	Price & Data Scraping, skewing of look-to-book ratio, denial of service, Price Scraping, Account Takeover

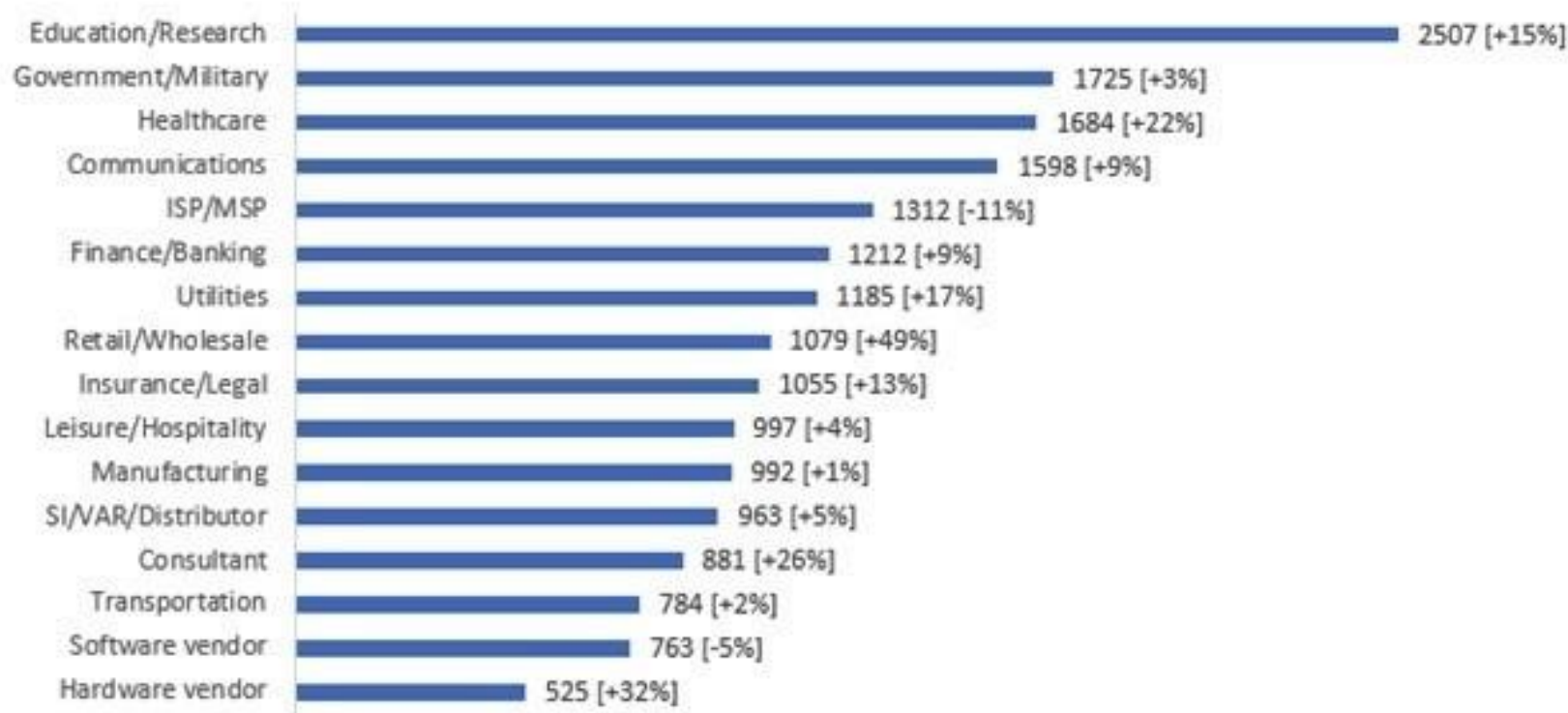


Common  
misconceptions...



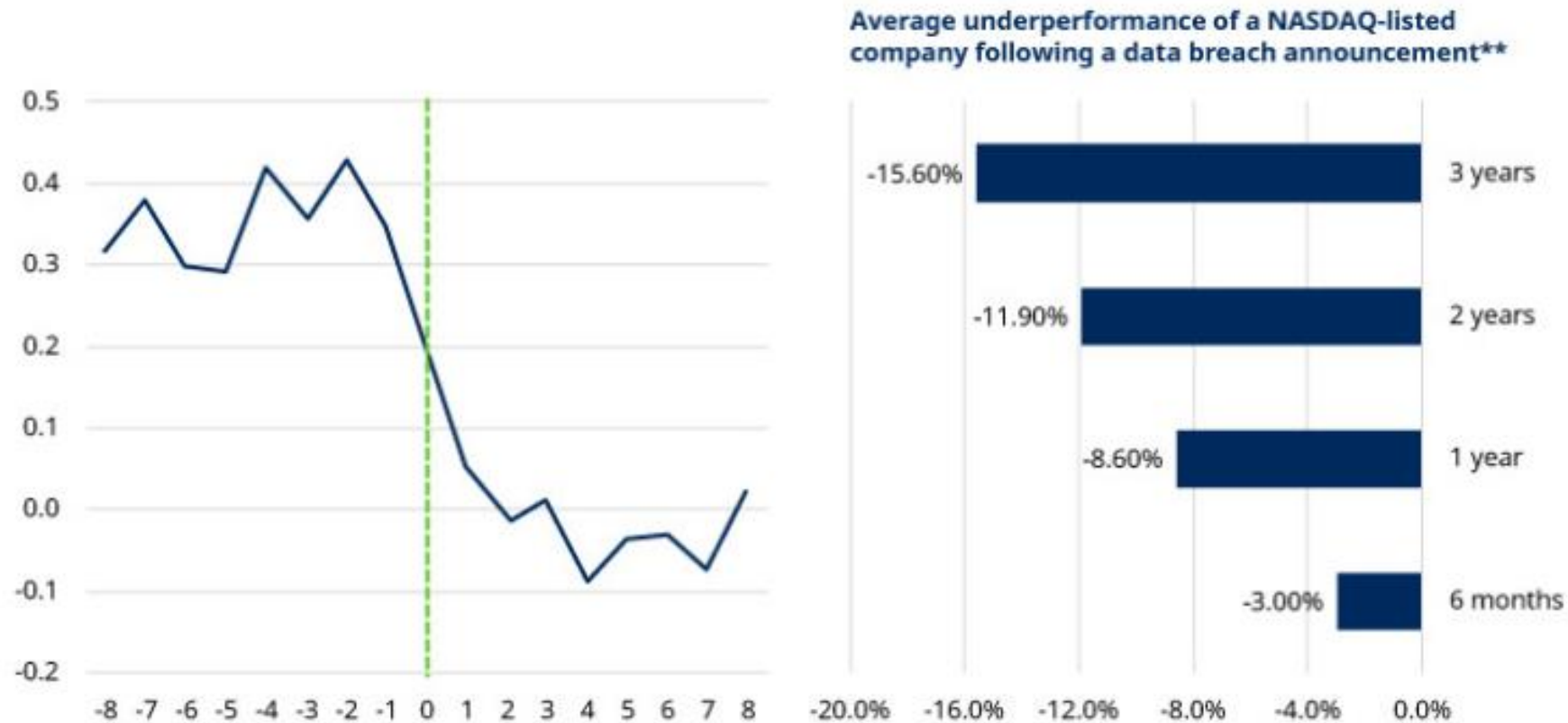
## “My industry is safe”

Global Avg. Weekly Cyber Attacks Per Industry  
(2022 Q1 Compare to 2023 Q1)





“My company is large enough to handle it”



Source: Rotman School of Management. Note: \*Reputation rating based on a number of reputation risk issues.  
\*\*HSBC, Comparitech, Cybersecurity Ventures, Verizon, Munich Re. 602267

## “My company is too small to attack”



*Data breaches cost upwards of **£130,000** to fix.*



*64% of consumers are put off using a business that was the victim of a website compromise or data breach*



*60% of SME in the UK go out of business within six months of falling victim to a data breach or cyberattack.*

*Supply chain attacks are real.*

“Cybersecurity insurance will protect me”

Cyber attacks set to become ‘uninsurable’, says Zurich chief

FINANCIAL TIMES

DECEMBER 26, 2022

## Why should you care?

### To protect your business

1. Allowing potentially dangerous bot traffic on a website can result in an additional cyber threat – bots are actively looking for websites from which to steal data, break into accounts, set up fake accounts or to aid other forms of attack on your company, including phishing.
2. Malicious actors (or competitors) may be scraping your data to pretend to be you, risking your hard-earned brand position.
3. Competitors may be engaging in basket blocking – stopping you selling to your customers.
4. You might lose hundreds of thousands or millions in revenue if your website is compromised or offline.
5. Regulators may fine you for breach of data
6. Detecting and removing malicious bots from ad campaigns means that cyber risk is reduced, and active bots are less likely to find and attack your website.

### To gain better results

1. Malicious bots are trying to appear human, which means they get served digital ads (costing you in CPM) and interact with ads (costing you in CPC).
2. Your competitors may be buying bot traffic to waste your digital ad budget and improve their ranking and handing them an advantage over you.
3. Reducing or removing impressions and clicks from non-human traffic will improve campaign effectiveness at the top of the funnel: more humans, less bots. You better understand what is happening.
4. Why pay for traffic that is of no use to you? Removing bots is budget saving.

# Phishing protection for the legal sector

## The Bot Defence Experts



## Phishing

‘Phishing’ is when criminals use scam emails, text messages or phone calls to trick their victims. ‘Vishing’ is similar but uses voice or video calls, often using Generative AI to simulate a trusted contact.

A phishing attack is more likely to succeed if it appears credible. One of the best sources of data available to attackers for this information is your website.

*Phishing is one the primary ways in which attackers access an organisation to steal data or commit some other form of fraud.*

## Phishing

The UK Government's "Cyber Breaches Survey" 2023 found that of the 48% of UK businesses who identified a cyber-attack, the most common threat vector was phishing attempts (79%).

The "Singapore Cyber Landscape" 2022 report, published by the CSA, noted that phishing attacks more than doubled from 2021 to 8,500 reports in 2022 in Singapore.



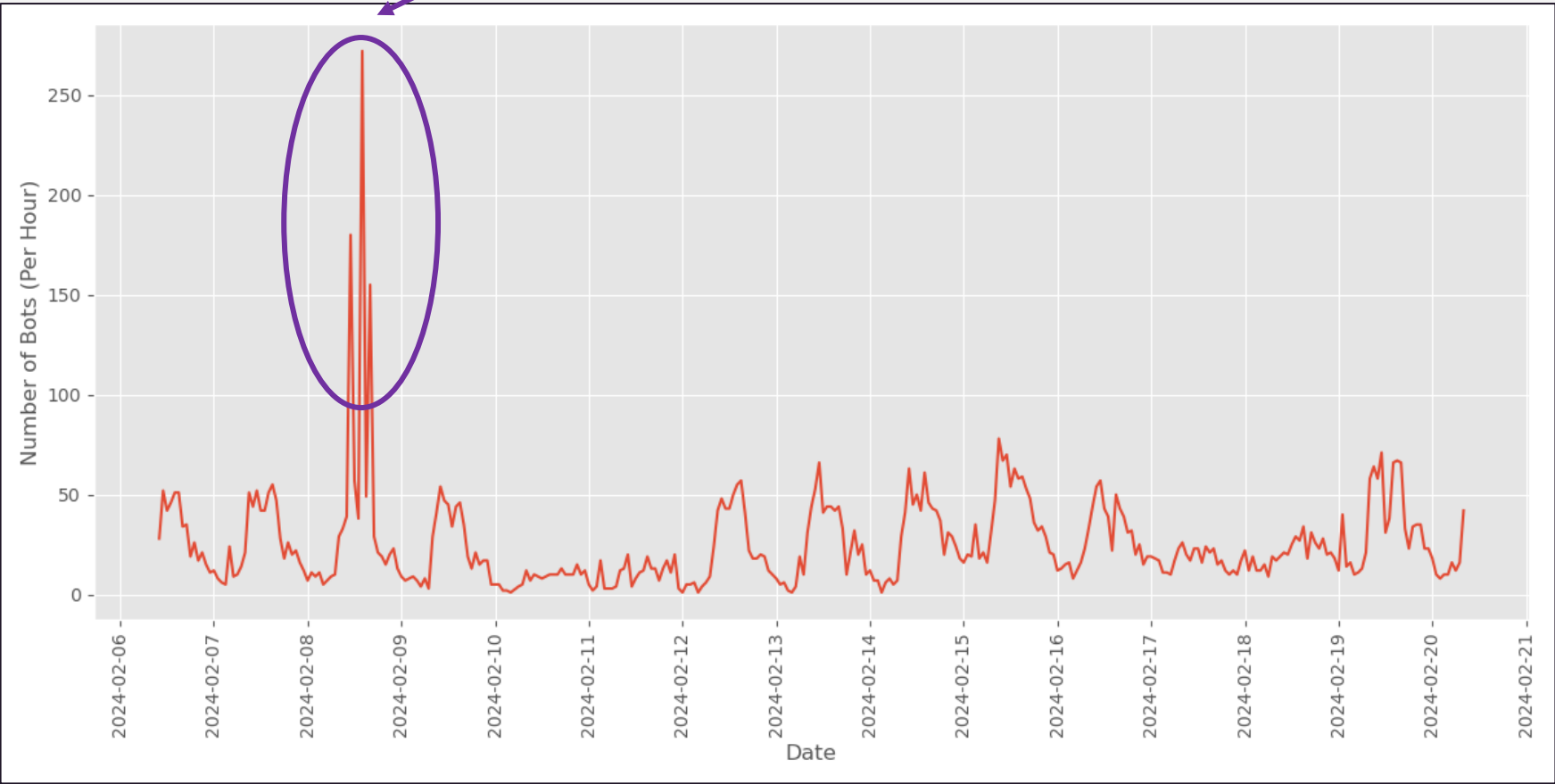
“



Organisations in the legal sector routinely handle large amounts of money and highly sensitive information, which makes them attractive targets for cyber criminals. Firms are vulnerable in new ways due to changing patterns of work – accelerated in the COVID-19 pandemic – and the increasing sophistication of cyber-attacks.

Lindy Cameron – CEO NCSC // Foreword to “Cyber Threat Report: UK Legal Sector” 2023

Targeted "phishing data gathering" bot attack



*Bot levels Over Two-Week Period*

# Phishing protection for the legal sector

## The Bot Defense Experts



HERE

THERE

EVERYWHERE

# In Summary

## Your digital assets will be attacked

- › for your **data**
- › for your **customer's** data
- › for **money**
- › for information that might be **useful** elsewhere
- › for whom you do **business** with, and who they do business with
- › because you might **pay** to have your website or data back
- › because bots want to look **human**
- › because it's **easier** to attack a website or mobile app
- › because it's **fun**
- › **because** you happen to be there

“Technology will exacerbate inequalities while risks from cybersecurity will remain a constant concern.”

[WEF\\_Global\\_Risks\\_Report\\_2023.pdf \(weforum.org\)](https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf)

[https://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2023.pdf](https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf)



“The biggest issue in the Cybersecurity Industry is the ever-evolving nature of cyber threats...”

AiSP President Mr Tony Low, April 2024





## The Bot Defense Experts

The risk from malicious bots is genuine and real.

It is not an acceptable answer to have no visibility of the impact of bots on your web estate.

Understanding, mitigating and removing bots increases an organisation's security profile and adds value to the whole business.

Connect with Stewart Boutcher

Global CTO, APAC CEO

<https://www.linkedin.com/in/thebluehand/>