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

Veracity Trust Network

https://veracitytrustnetwork.com/

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

1. Introduction: what is cybersecurity?
2. What is a bot?
3. How might this impact you?
4. Detecting bots is difficult.
5. Summary & next steps.

GET YOUR PHONE READY – QR CODE HEAVEN AHEAD

Introduction:
What is Cybersecurity?

Veracity Trust Network

https://veracitytrustnetwork.com/

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks

people

Employee awareness, behaviours and training.

Specialist skills, experience and qualifications.

Appropriate staffing levels to manage and monitor environments.

process

Effective management systems and policies.

IT governance, risk, and compliance using framework such as Cyber Essentials, ISO 27001 and SOC2.

Security audits and gap analysis.

Response and disaster recovery plans.

technology

Network, infrastructure and platform security.

Endpoint security, detection and response.

Application and software security.

Vulnerability scanning and monitoring.

Advanced threat protection.

Identify and access management.

Managed security solutions and services.

Data security and protection.

Cloud security.

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

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

"The biggest issue in the Cybersecurity Industry is the ever-evolving nature of cyber threats…"

President Mr Tony Low, April 2024
Singapore based Association of Internet Security Professional (AISP)

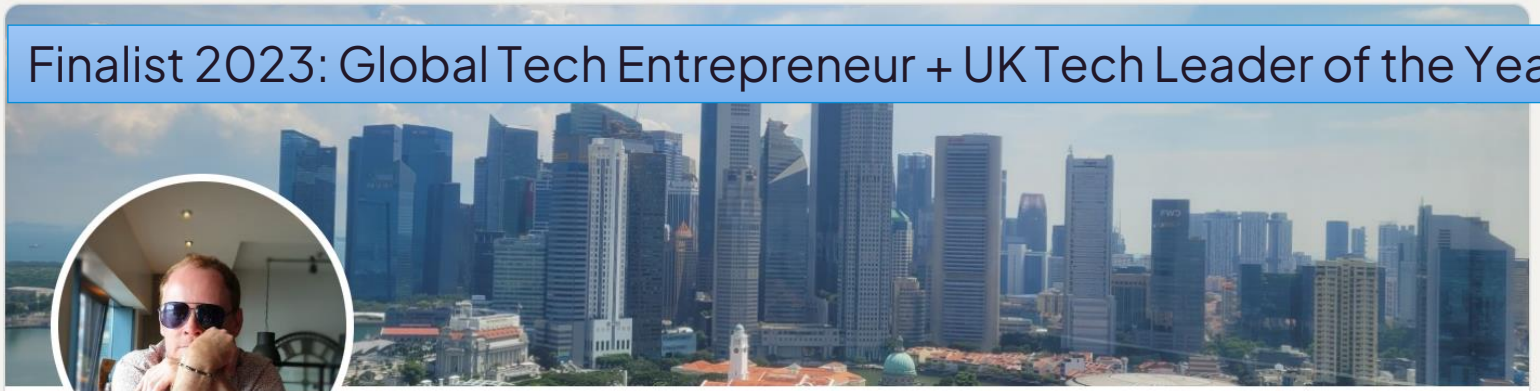
Malicious Bots: Protecting your Digital Business from the Foot Soldiers of Modern Cyber Attacks

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

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



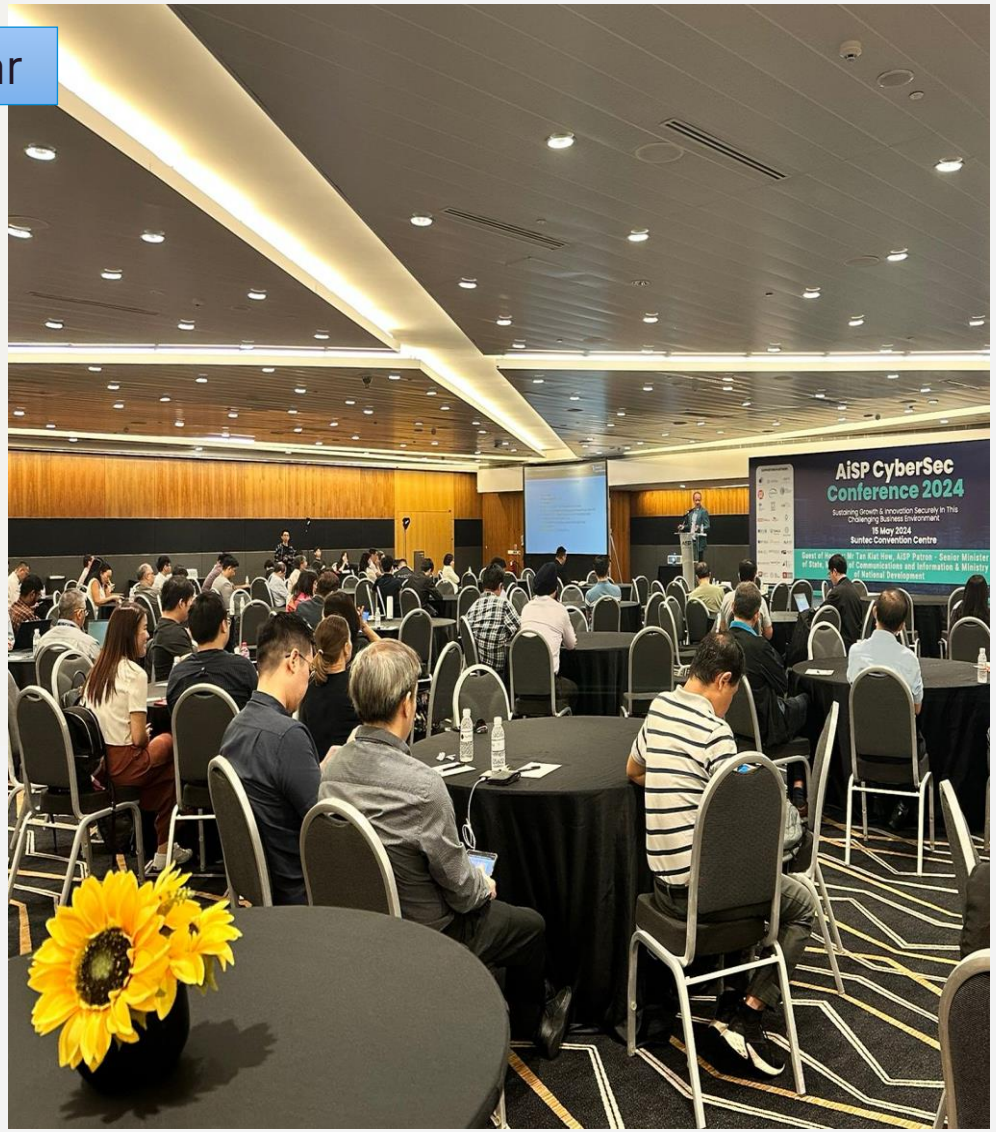
Stewart Boutcher (He/Him)

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.

Greater Leeds Area · Contact info

Veracity Trust Network

Aberystwyth University



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.

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

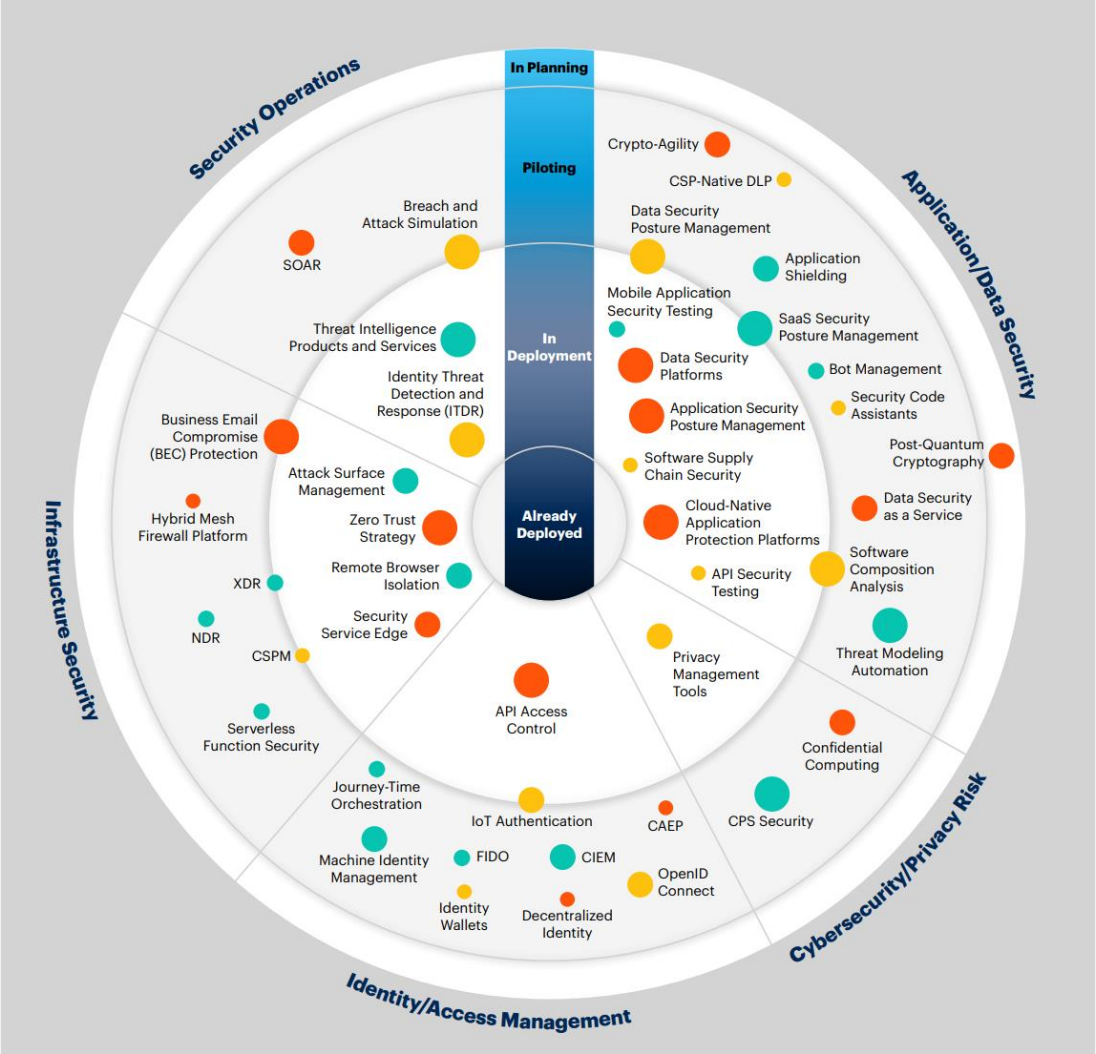
"AI algorithms can optimise attack strategies by analysing network vulnerabilities, evading detection mechanisms, and exploiting weaknesses in real time…This enables them to develop new attack techniques at an alarming pace"

Stewart Boutcher, CTO Veracity Trust Network.

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

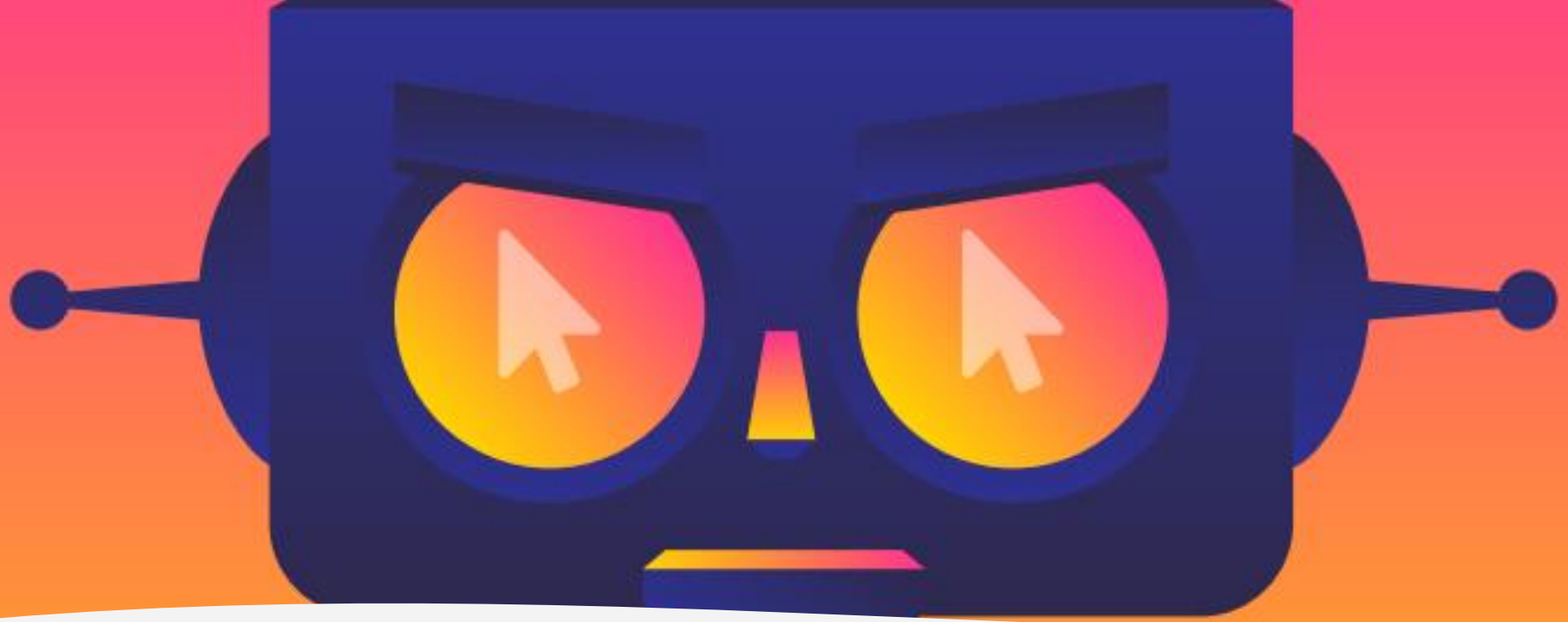
Veracity Trust Network

Where bot protection fits into cybersecurity



Gartner

"2024 Technology Adoption Roadmap for Security and Risk Management"



How might it impact you?

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

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

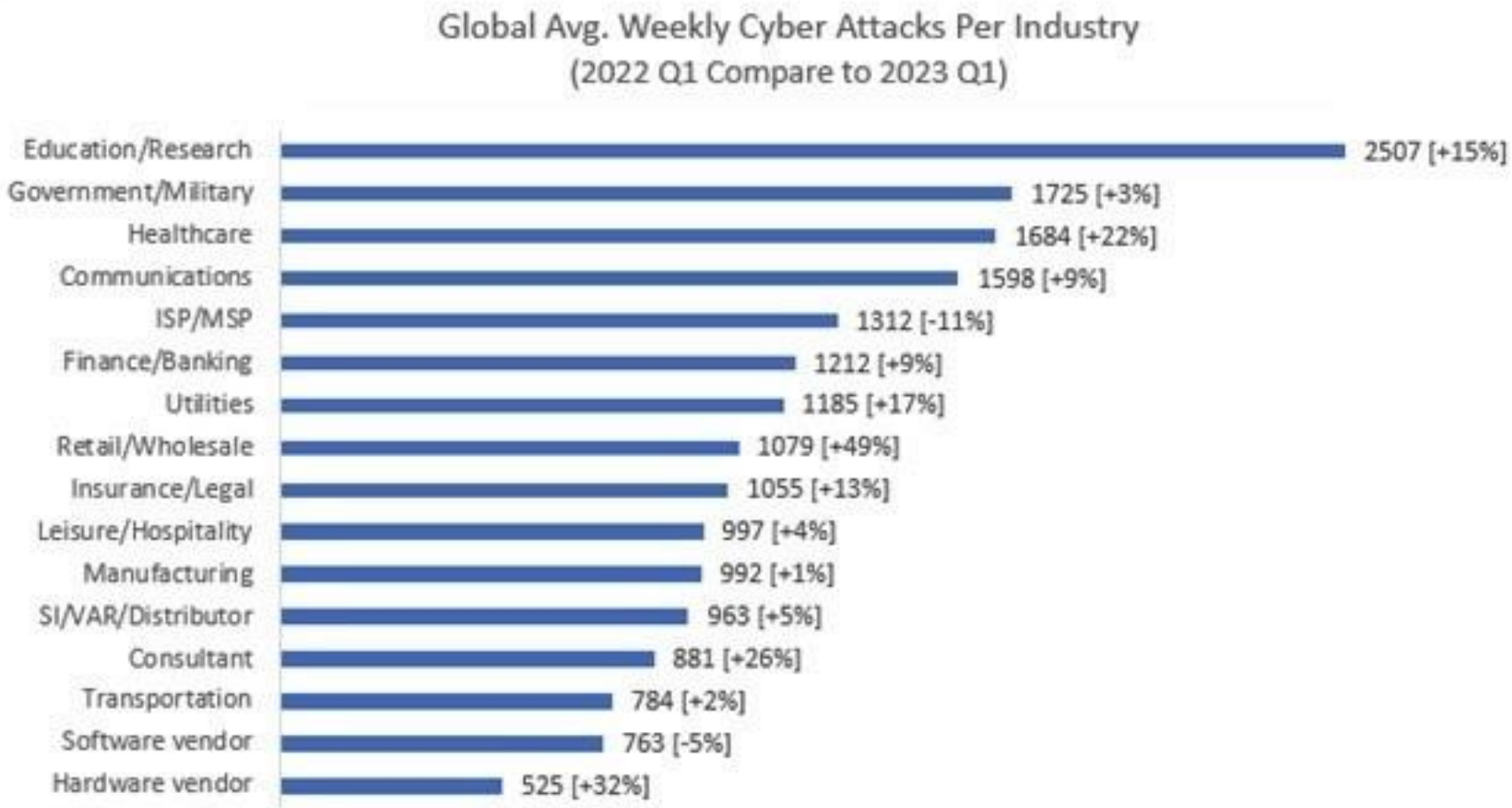
Common misconceptions…

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

"My industry is safe"



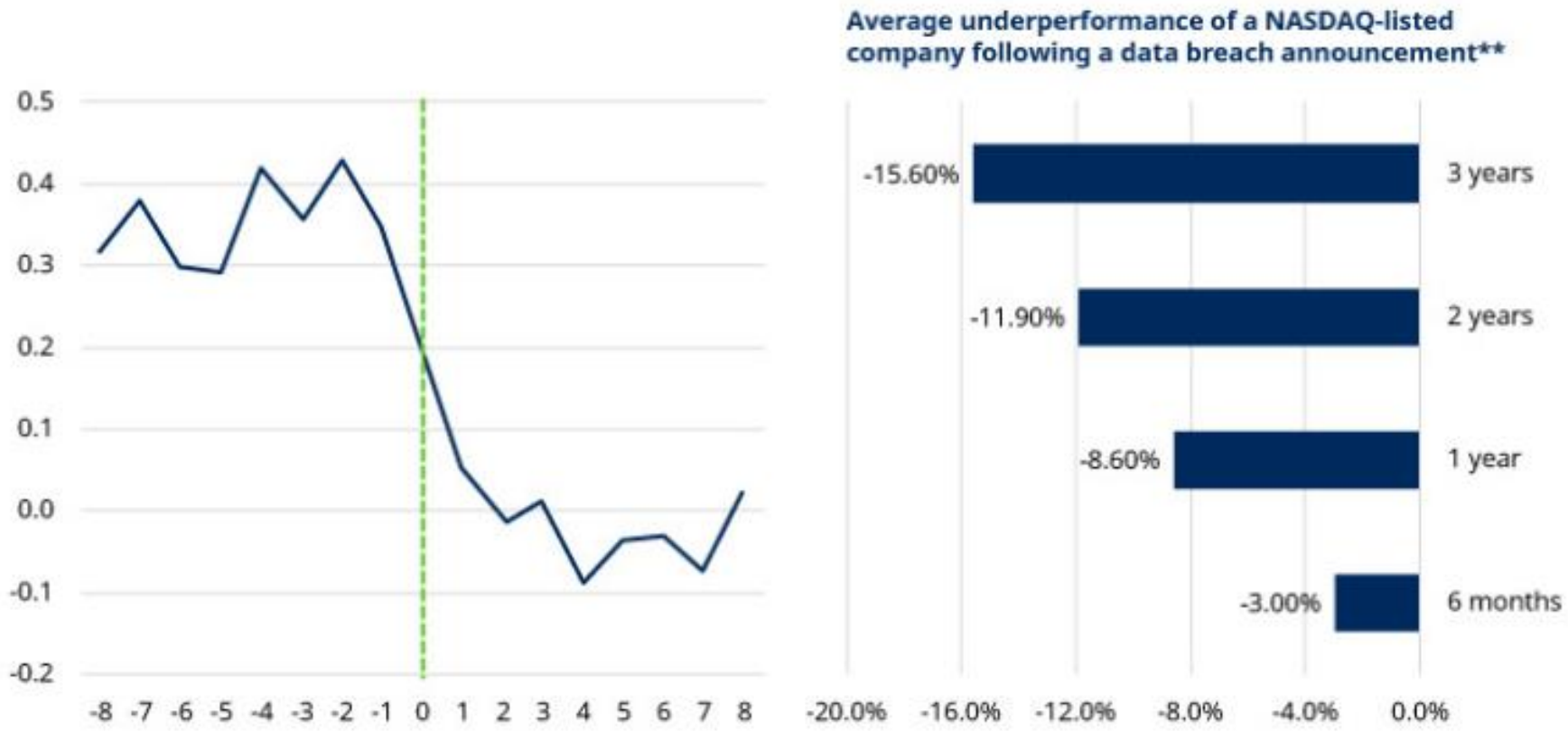
WORLD ECONOMIC FORUM

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

"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

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

"My company is too small to attack"

National Cyber Security Centre

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

experian

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

National Cyber Security Centre

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.

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

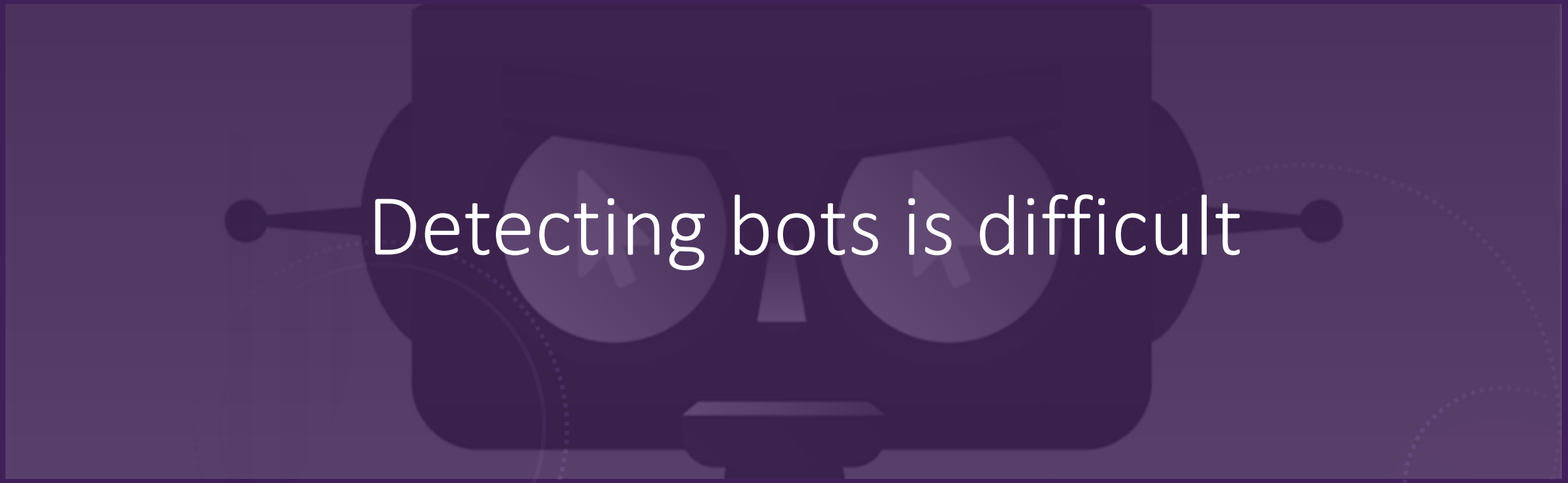
"Cybersecurity insurance will protect me"

Cyber attacks set to become 'uninsurable', says Zurich chief

FINANCIAL TIMES

DECEMBER 26, 2022

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

“

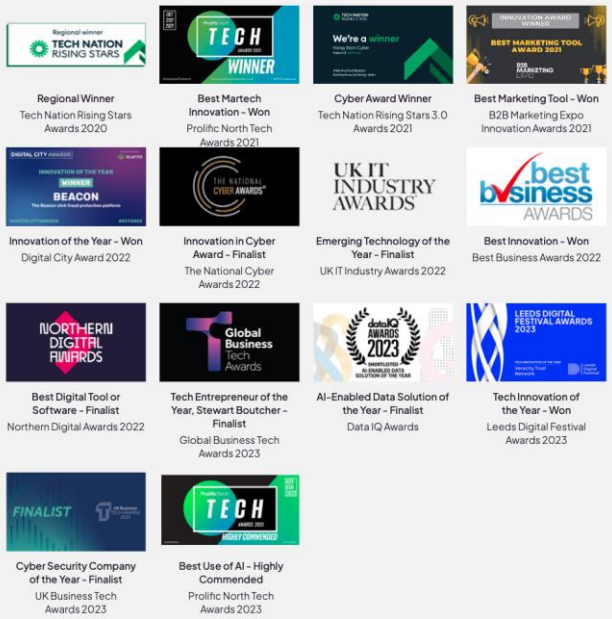
Part of the reason sophisticated bot attacks can be hard to stop is due to the complexity inherent in intelligent bots…reactive fraud solutions that rely only on known patterns and historical data are fairly ineffective, because fraudsters use AI to evade detection and present signals meant to deceive most bot detection systems.

The Intelligent Bot Revolution: What Businesses Need To Know

Veracity Trust Network

https://veracitytrustnetwork.com/

The Bot Defense Experts



CYBER RUNWAY SCALE BY plexal ALUMNI

Department for Science, Innovation, & Technology

Shortlisted as:

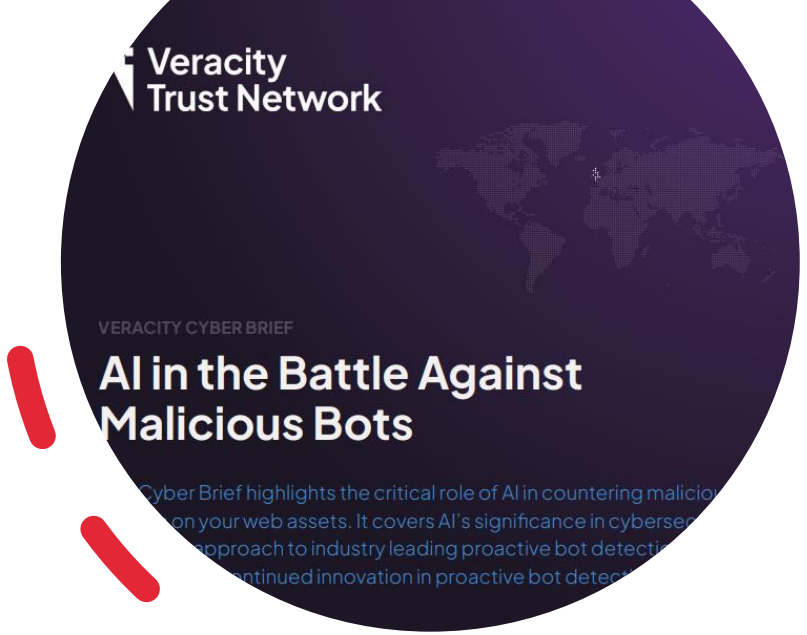
UK's Most Innovate Cyber SME 2024

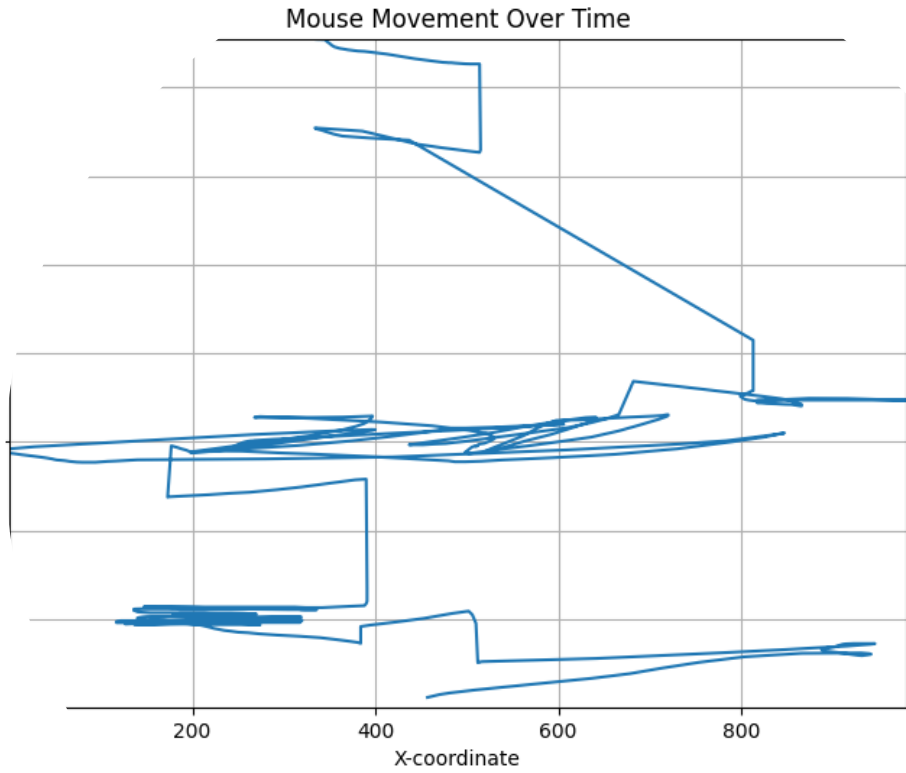
amazon web services Partner Network
TECHNOLOGY PARTNER

AiSP Advance Connect Excel

Infosecurity® Europe
4 - 6 June 2024, ExCeL London

- 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.





Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

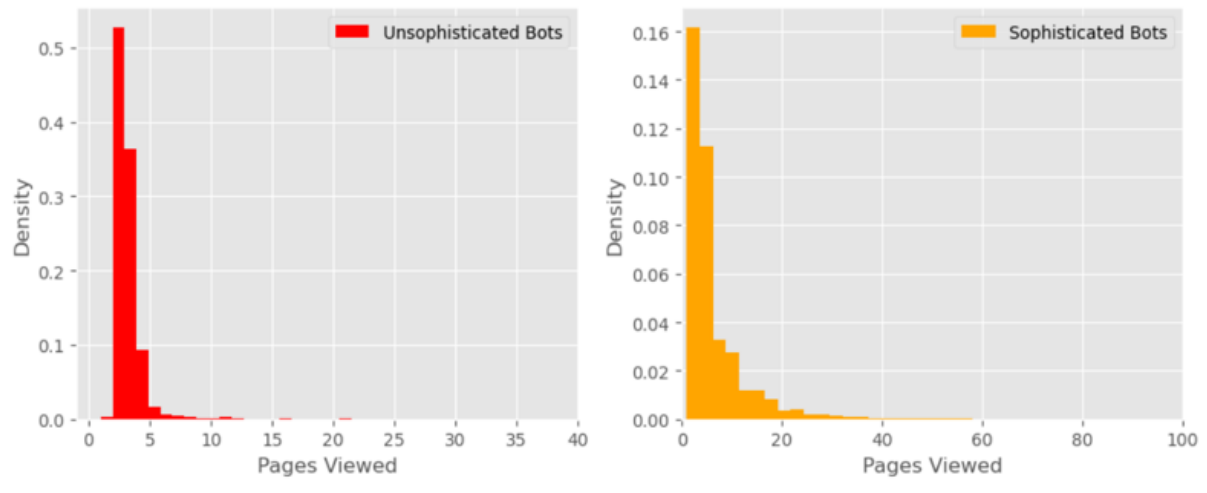


Figure 6: Difference in Pages Viewed Between Sophisticated and Unsophisticated Bots

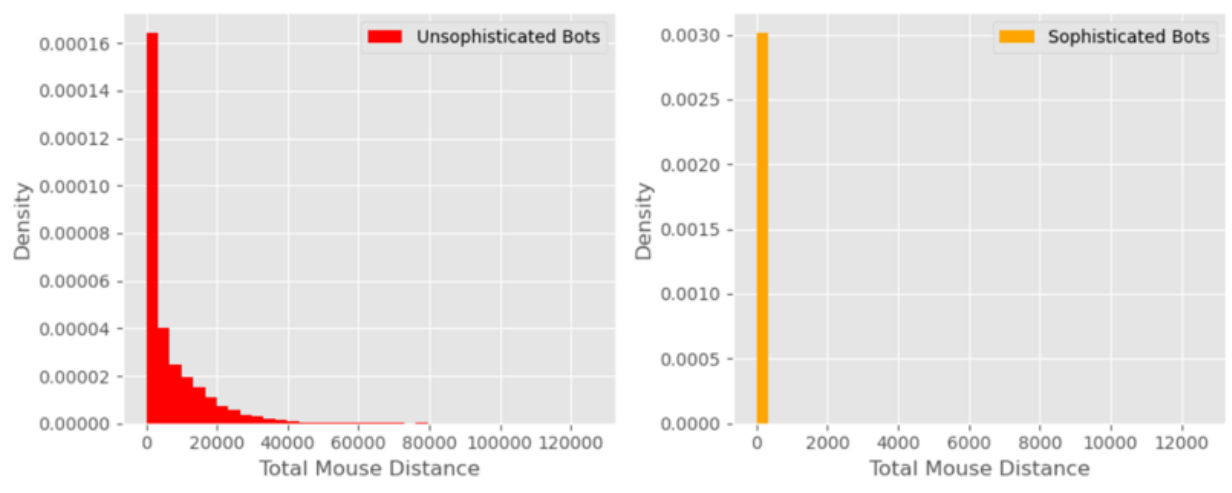


Figure 7: Difference in Total Mouse Distance Between Sophisticated and Unsophisticated Bots

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

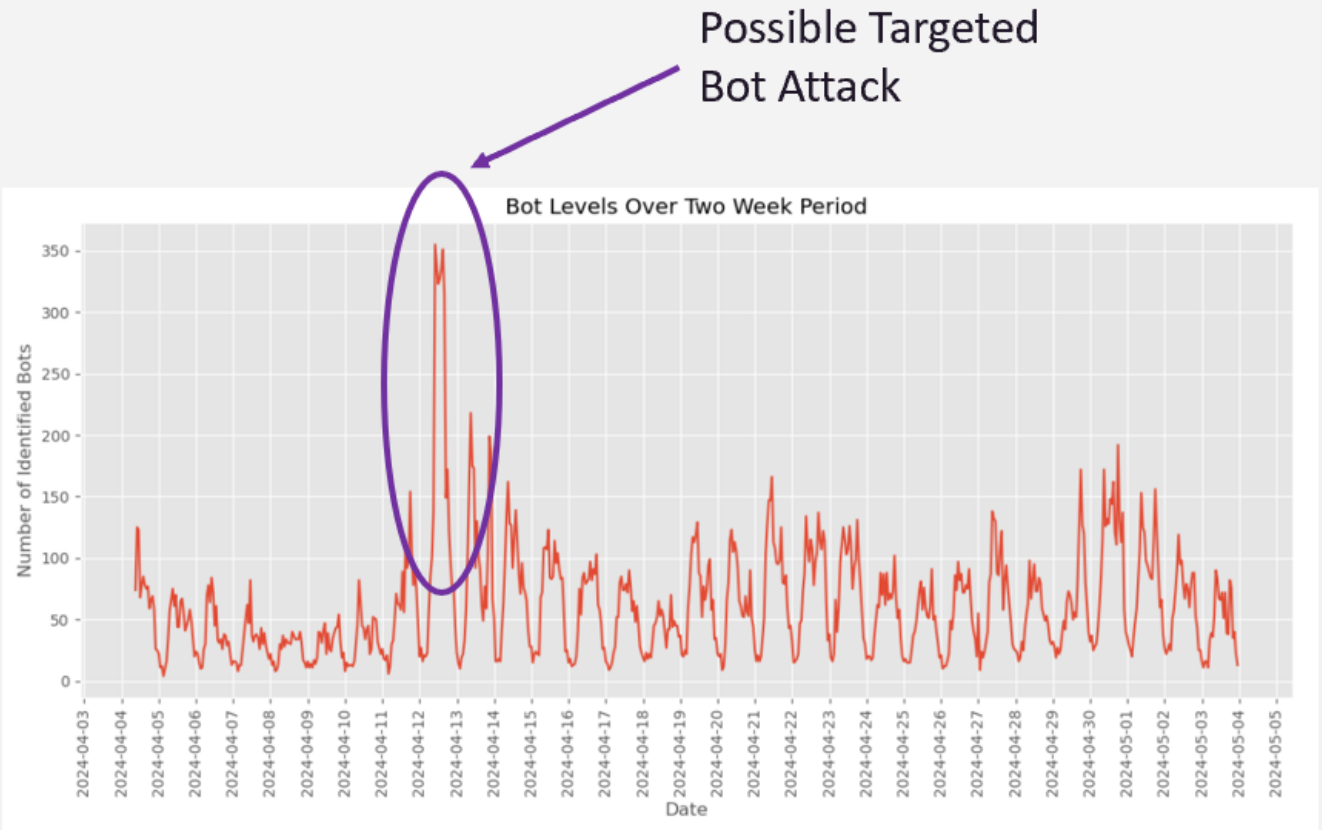


Figure 8: Bot Levels Over Month-Long Period

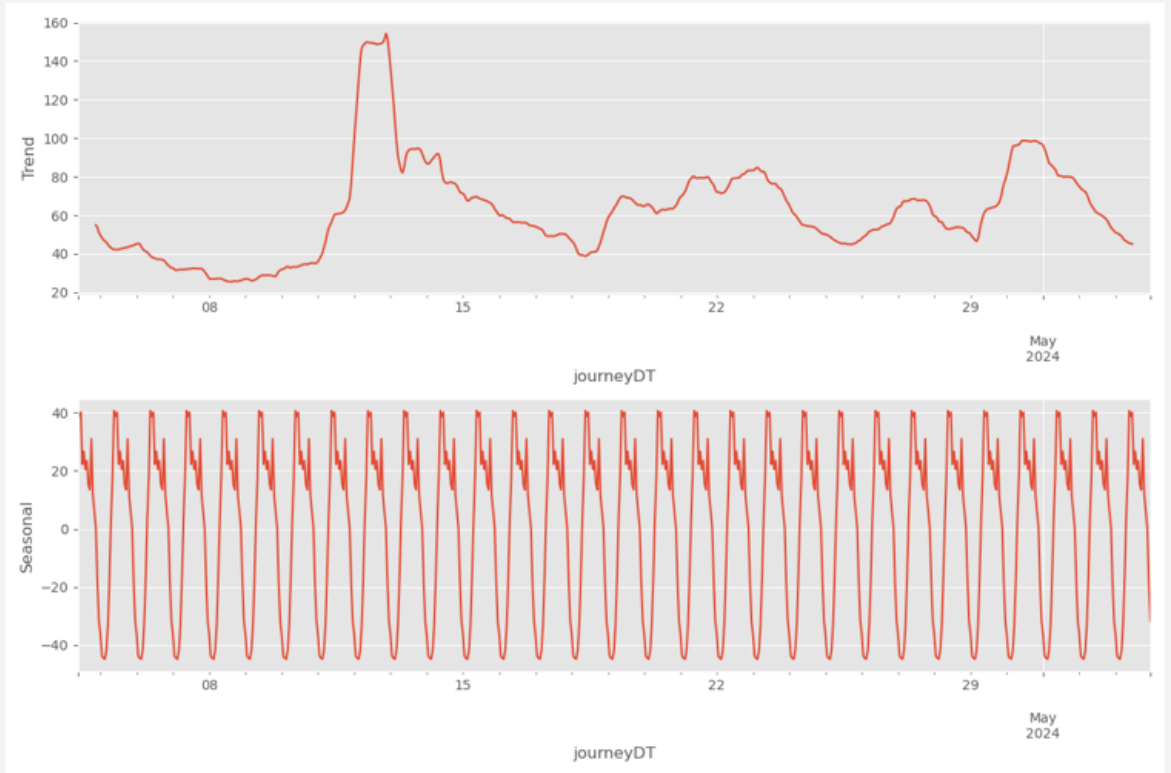


Figure 9: A Time Series Analysis Showing the Trend and Regularity of Bot Levels

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

In Summary

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

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

Stewart Boutcher, CTO Veracity Trust Network.

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

Veracity Trust Network

Protecting your public digital assets from bots is key

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.

Veracity Trust Network

https://veracitytrustnetwork.com/

Case Study –

Phishing protection for the legal sector

Veracity Trust Network

https://veracitytrustnetwork.com/

Get involved –
The Cybercast Sessions