RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **AIR2-M06**

Automated Threats: The Rise of Bots and What to Do About It

Matthew Gracey-McMinn

Head of Threat Research
Netacea
@MGM_Cyber

Simon Goldsmith

Director of Information Security
Ovo Energy
@CyberGoldsmith

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

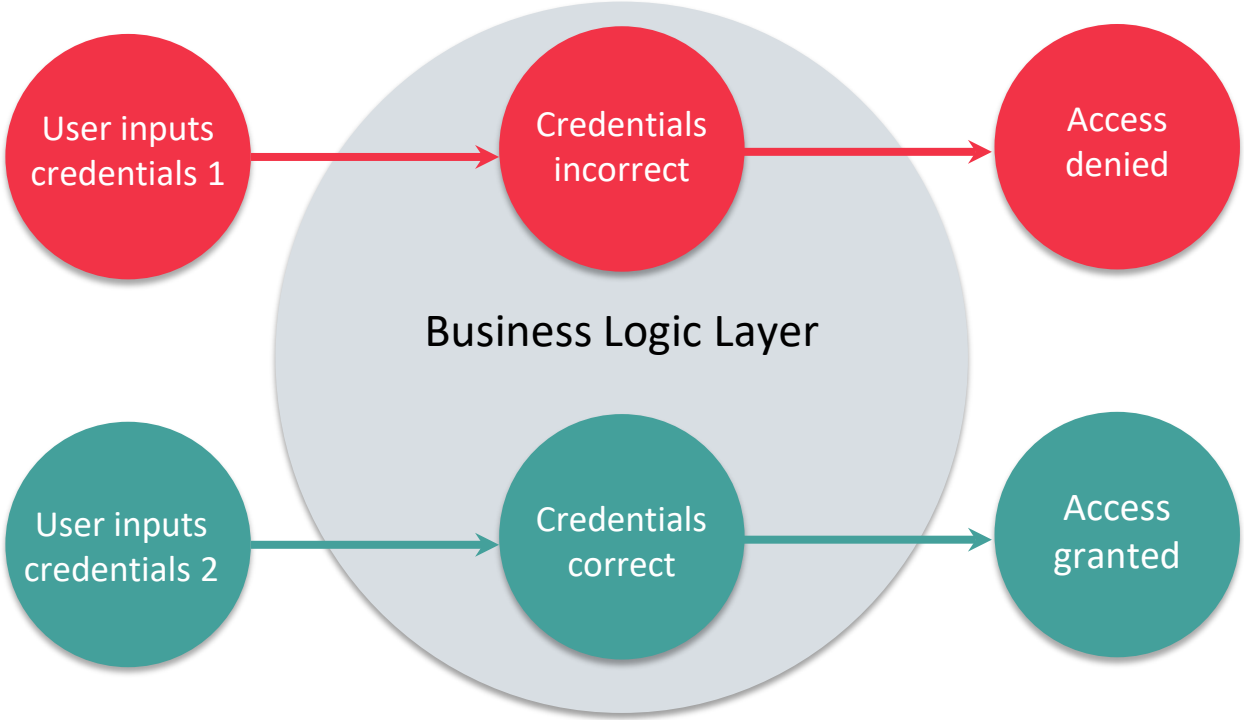
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

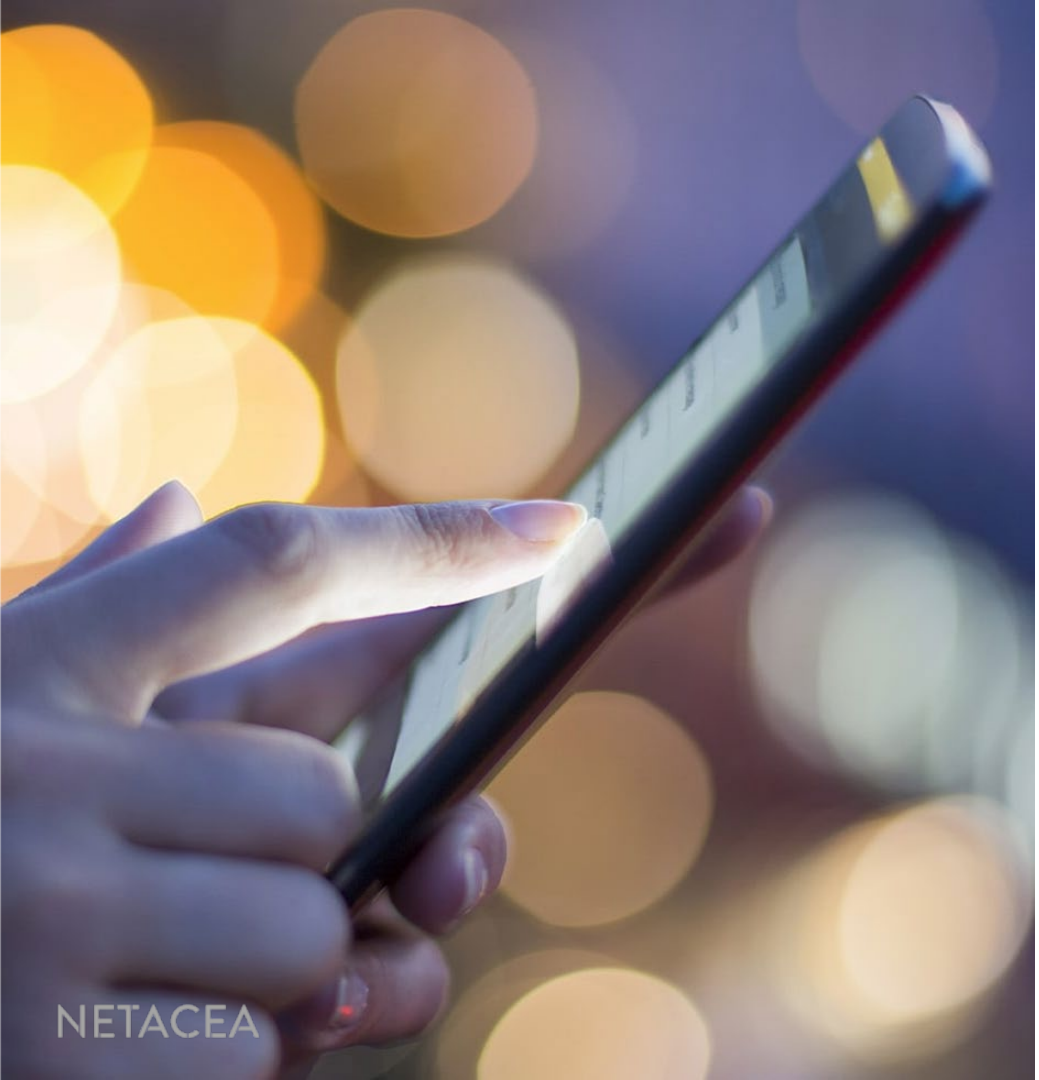
RSAConference2022

Why should I care about Business Logic Attacks and Bots?

What is Business Logic?

- The programming that manages interactions between an end-user application and a database

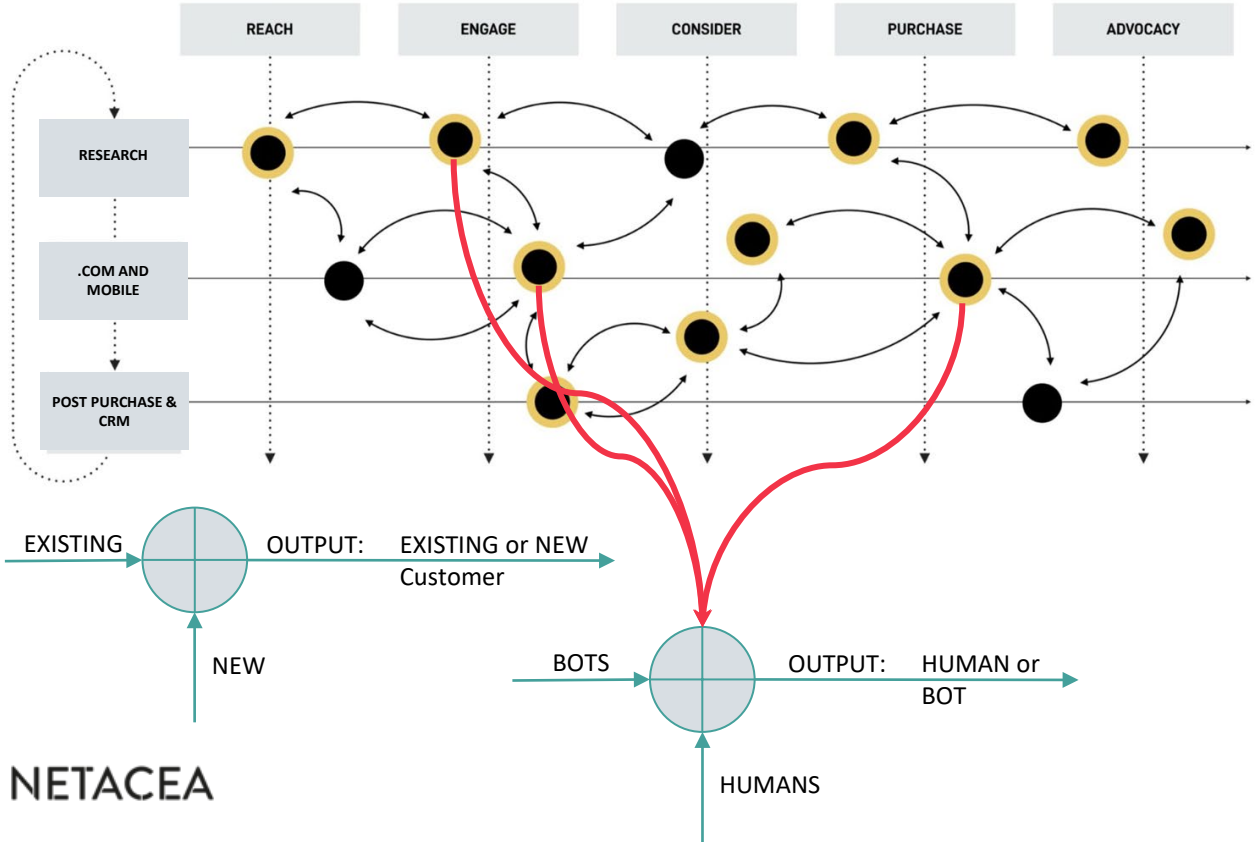




Business logic is digital now

Engaging consumers in a premium, personalised and connected digital brand experience across all our consumer touch points in the digital ecosystem

Business Logic In Action: Customer Experience

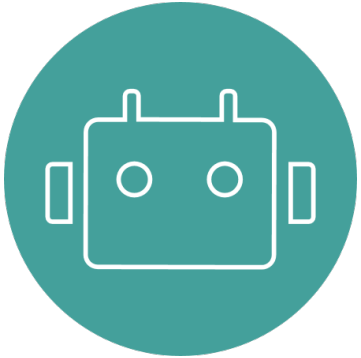


Example:

1. Stimuli that intrigues
2. Research the stimuli
3. Explore .com
4. Browse and compare others
5. Remarketed via social media
6. Login/Sign Up/Download App
7. Purchase completed
8. Purchase shipped
9. Purchase received
10. Product reviewed and recommended

‘Hacking’ vs business logic attacks

Hackers exploit technical weaknesses in your web-facing systems



BLAs use legitimate activity to exploit business logic weaknesses within your website

Bots & business logic attacks

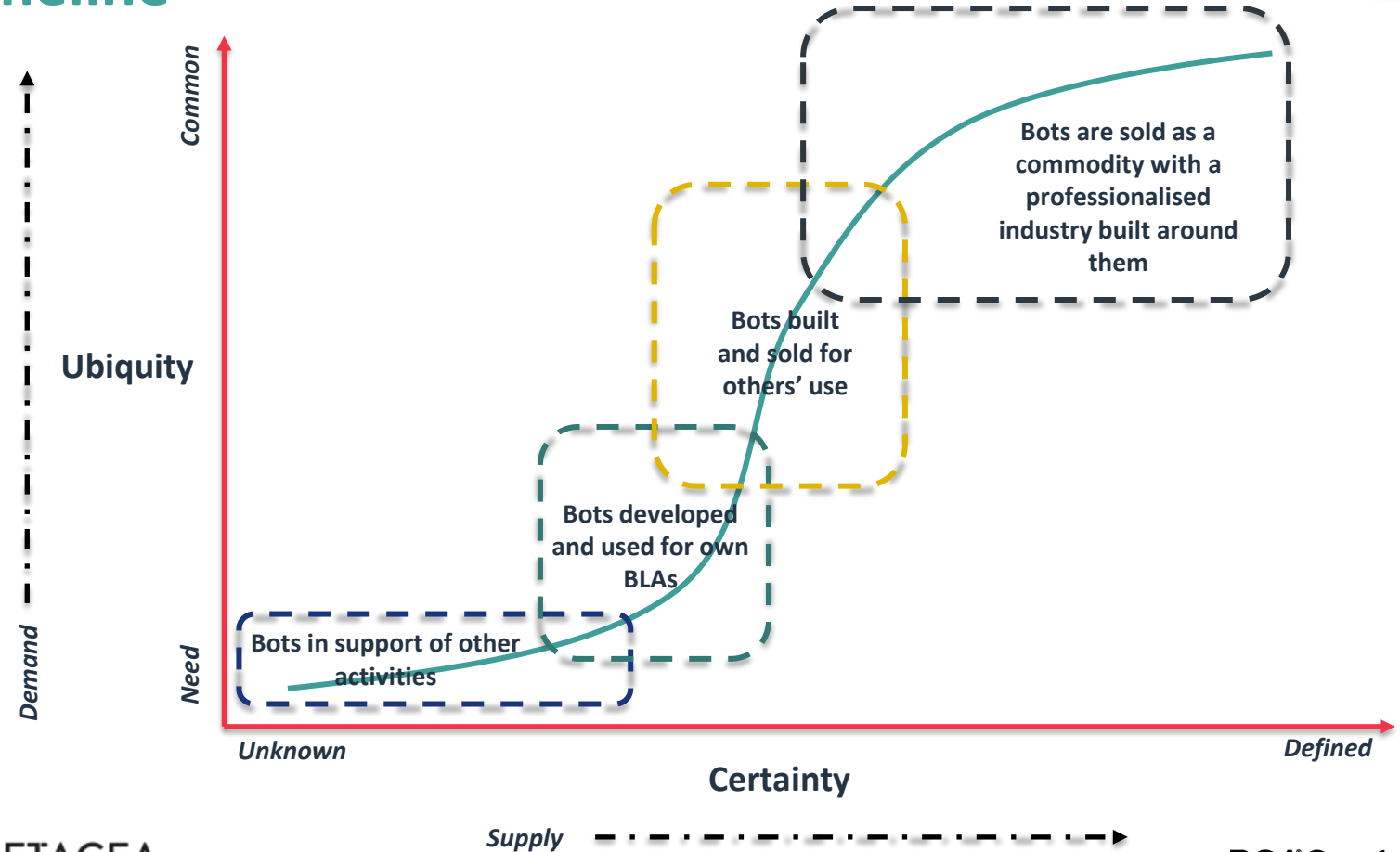
Good bots

- Search engines
- Uptime checker
- Security scanners
- SEO tools
- Partner services
- Content aggregator
- Price comparison

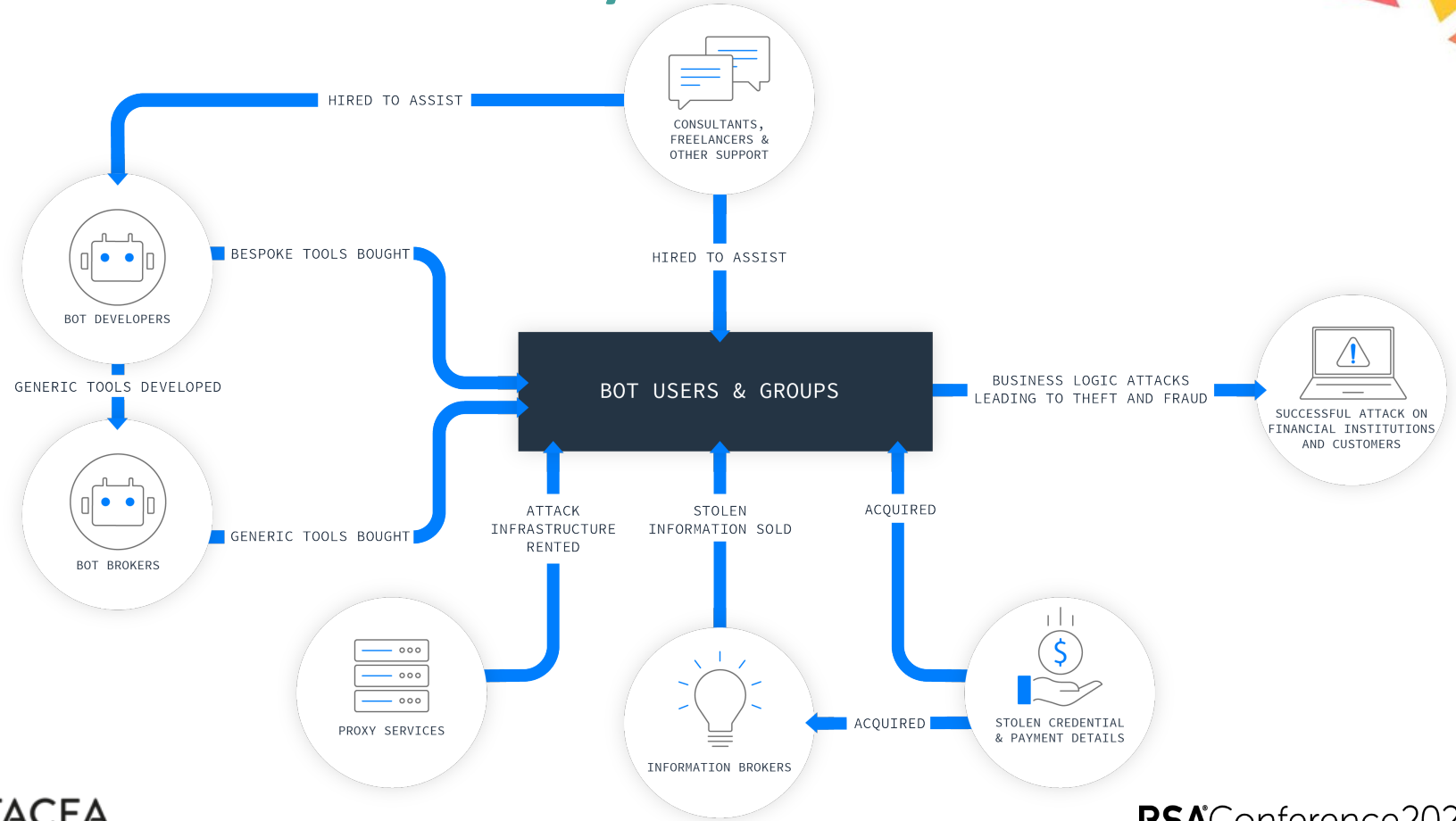
Bad bots

- Credential stuffing
- Sniper
- Fake account creation
- Carding
- Scraping / content harvesting
- Scalper
- Spinner

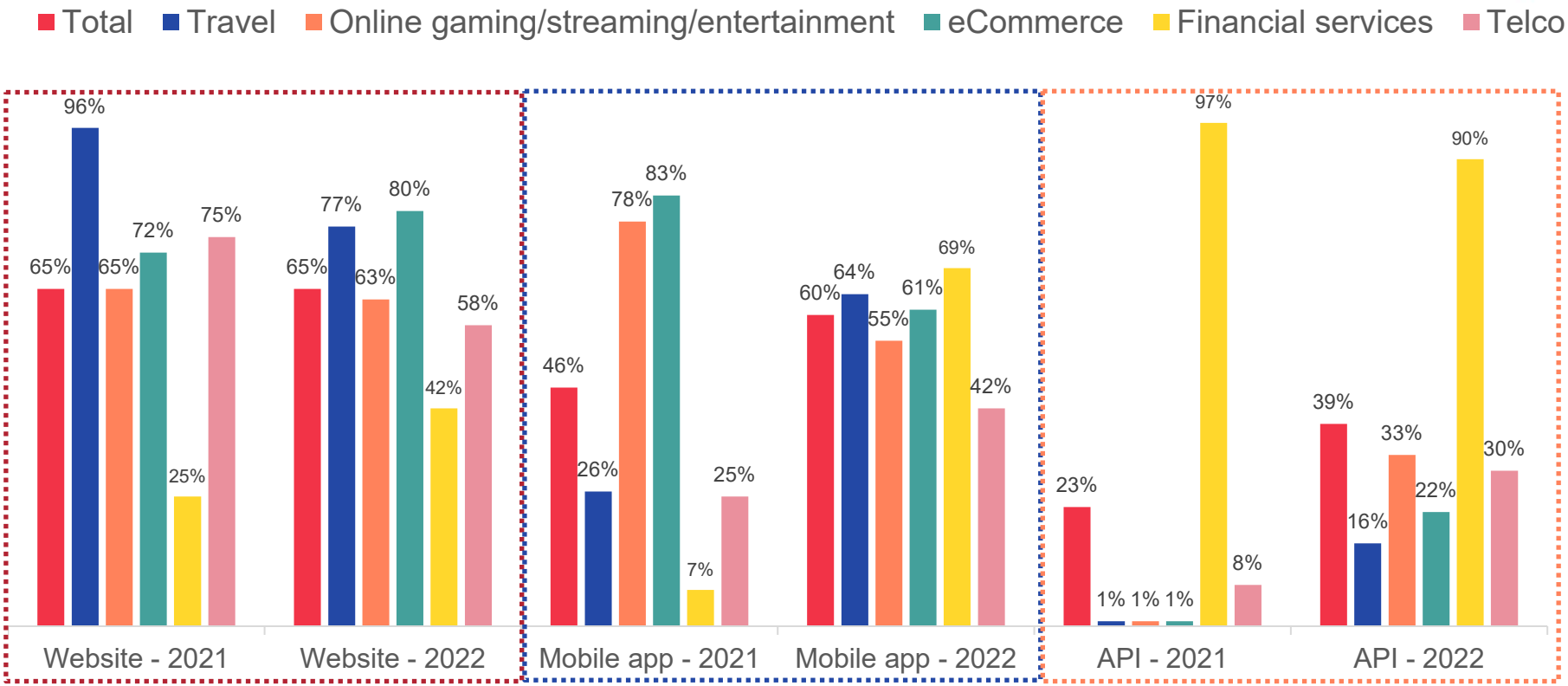
Timeline


Common
Ubiquity
Demand
Need
Bots are sold as a commodity with a professionalised industry built around them
Bots built and sold for others' use
Bots developed and used for own BLAs
Bots in support of other activities
Unknown
Defined
Certainty
Supply

Financial Services Bot Ecosystem



Q. To your knowledge, which of the following have been attacked by a bot in the last year?

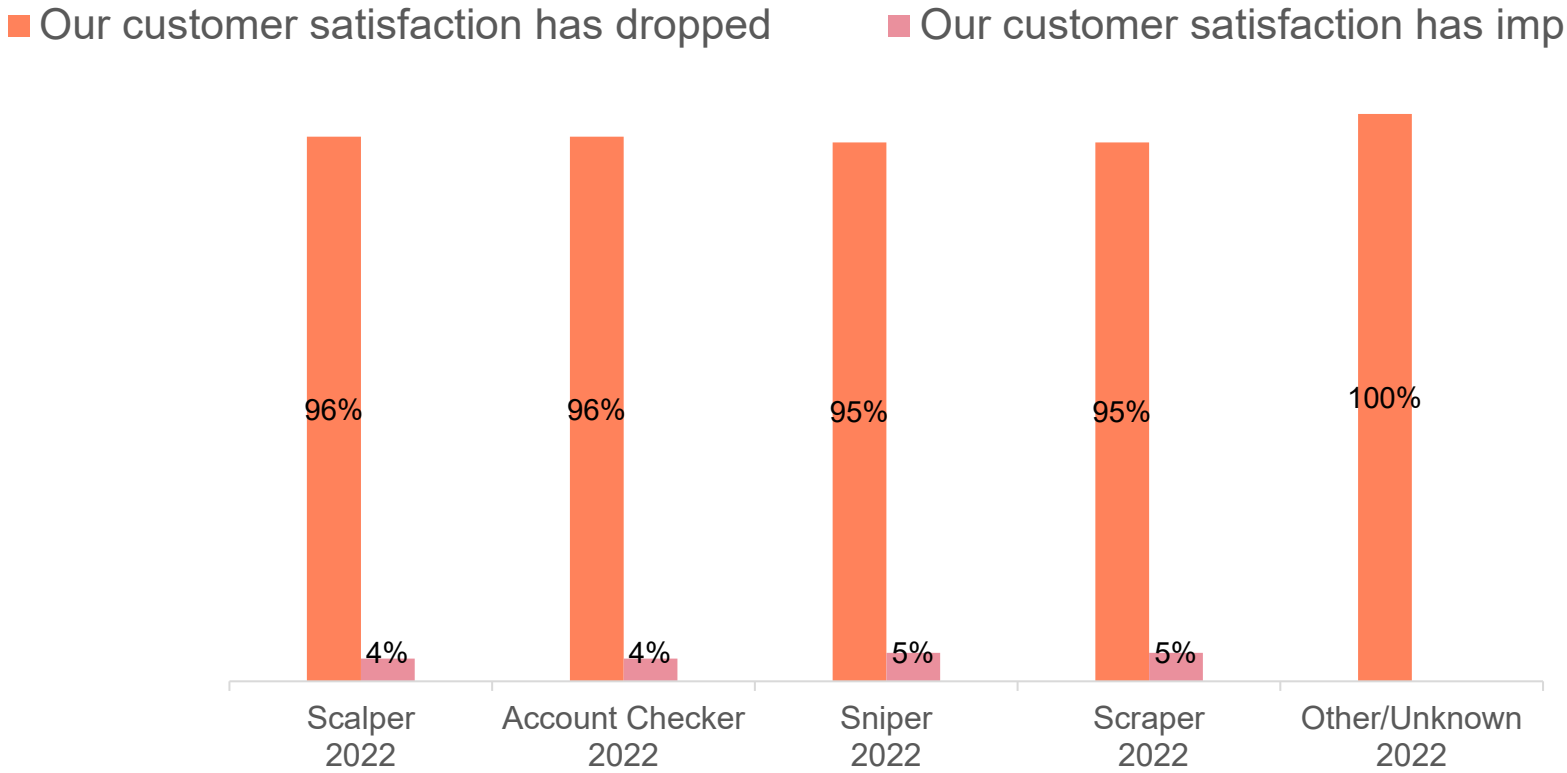


Key facts & figures (2022)

3.3% of annual revenue lost to bots on average

Equates to at least **$250 million** every year for top quarter of targeted businesses

Q. What impact have bot attacks had on your customer satisfaction?



Key facts & figures

16 weeks is the average amount of time taken to discover an attack has happened – up **2-4 weeks** from last year

8% of security budgets are allocated to bot management - up from **5%** last year

RSAConference2022

How do these attacks work?

The BLADE Framework

Phase	Tactic
Resource Development	Website Creation
	Credential Acquisition
	Infrastructure Acquisition
	Payment Detail Acquisition
	Tool Development
Reconnaissance	Loose Target
	Specific Target
Defence Bypass	Mitigation Bypass
	Human Emulation
	Proxying
	Smokescreening

Phase	Tactic
Attack Execution	Account Creation
	Account Takeover
	Fake Interaction
	Stock Purchase
	Spinning
	Sniping
	Policy Abuse
	Payment Detail Abuse
Actions on the Objective	Transaction Redirect
	Exfiltration

Phase	Tactic
Post-Attack	Invoice Abuse
	Delivery Redirect
	Resale

BLADE

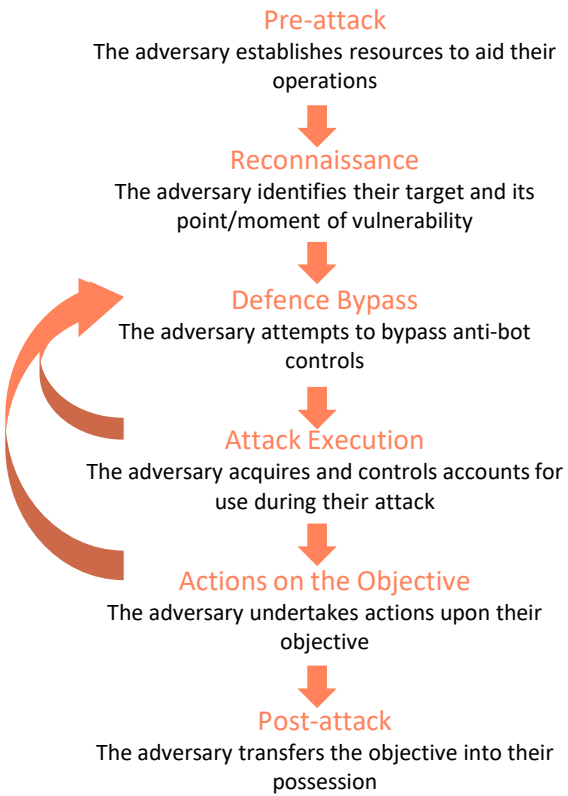
www.bladeframework.org

Live Demo

RSAConference2022

What should I do about all this?

BLADE Framework Usage



Example techniques

- Pastebin of stolen payment details from third party breaches
- Web scraping for product availability
- Automated captcha completion
- Fake account creation and automated purchase with stolen credit card
- Dumping of card details from successful payments – identifying usable stolen card details
- Redirection of shipped product to adversary location

Defense systems available

- Outside your control
- Perimieter Defences
- WAF
- Bot Management
- Fraud Prevention
- Manual Review

What to do next?

- Today:
  - Begin to understand the bot threat (check bladeframework.org)
  - Help build the community (@bladeframework on Twitter)
- Short-Term:
  - Threat Modelling
  - Check for indicators of business logic attacks (speak to other teams)
- Long-Term:
  - Design and implement a full bot management program

Questions?

The threat model is changing…