Business Logic Intelligence Service

NETACEA

If your business operates online, it is a target for criminal bot activity. Worse, criminals are increasingly focusing their bot attacks on specific businesses, making them much more dangerous.

Are your website's assets and user accounts for sale on the dark web? Illicit forums and marketplaces are so closely guarded that it's almost impossible to know how many stolen user accounts, digital assets or data leaks are exposed, let alone who is responsible.

Without this information, your security initiatives will be misdirected, leaving the business exposed to the most malicious threats. Yet dedicated in-house threat intelligence with the ability to infiltrate criminal bot communities requires highly specialized skills that are prohibitively expensive to resource, with bot intelligence often lacking from generic threat research services.

Netacea monitors billions of requests for the world's biggest sites, deconstructing bots continually. This gives us unmatched insights into their origins and tactics.

Customized threat intelligence directly related to your business

Netacea's Business Logic Intelligence Service is your secret weapon against even the most guarded threat groups. Our highly specialized professionals have successfully infiltrated criminal bot forums and communities, silently gathering intelligence about ongoing and new threats and the crooks responsible for them.

How we've helped our clients

- Tracking stolen user accounts on the dark web for a stock photo site
- Collecting evidence against adversaries in several ongoing legal cases
- Disassembling scalper bots so retail clients can detect their signals

Benefits of dedicated Business Logic Intelligence

- Focus intelligence to pinpoint on the biggest threats to your business
- React quickly to attacks by monitoring dark web activity
- Disrupt threat actors and fight back against attacks
- Assess the effectiveness of your defenses
- Free internal teams from the burden of specialized threat intelligence

Bespoke Intelligence Operations projects

As well as on-going reporting services, we can undertake bespoke Intelligence Operations to suit your needs. Potential assignments include:

- Dismantling a specific bot
- Disrupting a bot group or developer
- Support for legal action against an attacker
- And more – Contact us for details

NETACEA

Business Logic Intelligence Packages

Netacea offers fine-tuned Business Logic Intelligence services to suit the frequency and detail your organization requires, either as a stand-alone report or to augment your Netacea Bot Management solution.

Tier 1: Essentials

Essential threat research provided exclusively to all Netacea Bot Management customers.

Features

- ✓ Access to industry vertical trends
- ✓ Research into attacker capabilities fed into Bot Management service
- ✓ Contextualization of bot attacks to aid your response
- ✓ Access to our research library of whitepapers

Tier 2: Annual

Take the next step with active engagement in bot forums, collecting invaluable insights to bolster your defenses.

Features

Everything in Essentials, plus:

- ✓ Annual threat report
- ✓ Automated monitoring of bot forums and marketplaces
- ✓ Insight into specific threat groups targeting your business
- ✓ More detail on bot attacks against your sites, apps and APIs
- ✓ Red alert reporting on critical threats

Tier 3: Quarterly

Supercharge your threat research with active monitoring.

Features

Everything in Annual, plus:

- ✓ Quarterly threat report
- ✓ Active engagement in bot forums and marketplaces
- ✓ Comprehensive mapping of the threat landscape and how it changes over time
- ✓ Correlation of attacks seen by Bot Management solutions with specific groups

Tier 4: Monthly

Our top level includes an expert analyst integrated into your team, plus attacker disruption opportunities.

Features

Everything in Quarterly, plus:

- ✓ Monthly threat report
- ✓ Dedicated senior threat researcher integrated with relevant teams in your organization
- ✓ Identification of potential pressure points from which to disrupt your attackers