THE RACE FOR ONLINE TICKETS
...By Beating the Bots

Focus on the Business...

at a higher price at a later date.

can grab tickets. When the tickets are sold out, a fraudster can sell them

In this online ticket purchasing scenario, the deck is stacked against a

and Keep Malicious Bots Out!

Let Humans and Benign Bots in

Detecting Bot Attacks

Malicious Bots

Benign bots can benefit the business. Bad bots can break the business.

Detect human behavior, credit application fraud, impersonate identities and perform fraudulent transactions that could result in chargeback losses.

Leverage stolen credentials to automate large scale account takeover.

Collect and propagate information.

Leverage aggregators as a backdoor into other products, services, or company names referenced herein may be trademarks of their respective

For more information about how proactive, multi-layered bot protection can

provide human-like service through text or voice to responses.

Chatbots

Prevent excessive cloud charges

Prevent attacks that steal sensitive data

Protect current and potential customers:

Know the logic to Human Behavior:

Machine Learning (ML)

Adapt countermeasures while maintaining full efficacy

Identify and subtract points to a risk score. Then decide when and what type of action you

Assign risk scores to sessions with similar attack profiles and risk surfaces

Detect and block malicious bots without

human behavior.

uses bots and automation to imitate

Mitigate sophisticated fraud that

are increasingly being targeted by bots and

Protect mobile applications and APIs that

Be first to market but not first to breached:

Leverage stolen credentials to automate

Credential Stuffing

Identify

looks for suspicious behavior

Reverse Domain Name System lookup

Use CAPTCHA to challenge requests and

Issue a JavaScript challenge

Routing bot traffic.

Prevent attacks that steal sensitive data

Collect proprietary data that can lead to negative business outcomes like intellectual property theft.

Scraping

Crawl the Internet fetching data used

by search engines.

Search Engine Bots

Degrade performance and impact user experience

Impersonate identities and perform fraudulent

Credit Application Fraud

Perform money laundering via online banking

Fake Accounts

Abuse customer loyalty/reward programs.

Identify and steal gift card balances with value.

Gift Card Cracking

Identify automated script.

verify they are not from an automated script

automated attacks that use bots.

Extend defenses

restricted files or data using non-compliant searches

Restricted File Access

Determine if an HTTP request is coming from a search engine bot or customer, a search engine bot part that could improve SEO, or is this bot part

of an automated credential stuffing attack that may lead to account takeover, attacker arsenals. The question becomes intent – is this a human and potential

intelligence and customer engagement. Bots also reduce costs and scale

Bots reduce costs for basic and repetitive tasks and can improve business

Detecting Bot Attacks

Malicious Bots

Benign bots can benefit the business. Bad bots can break the business.

Detect human behavior, credit application fraud, impersonate identities and perform fraudulent transactions that could result in chargeback losses.

Leverage stolen credentials to automate large scale account takeover.

Collect and propagate information.

Leverage aggregators as a backdoor into other products, services, or company names referenced herein may be trademarks of their respective

For more information about how proactive, multi-layered bot protection can

provide human-like service through text or voice to responses.

Chatbots

Prevent excessive cloud charges

Prevent attacks that steal sensitive data

Protect current and potential customers:

Know the logic to Human Behavior:

Machine Learning (ML)

Adapt countermeasures while maintaining full efficacy

Identify and subtract points to a risk score. Then decide when and what type of action you

Assign risk scores to sessions with similar attack profiles and risk surfaces

Detect and block malicious bots without

human behavior.

uses bots and automation to imitate

Mitigate sophisticated fraud that

are increasingly being targeted by bots and

Protect mobile applications and APIs that

Be first to market but not first to breached:

Leverage stolen credentials to automate

Credential Stuffing

Identify

looks for suspicious behavior

Reverse Domain Name System lookup

Use CAPTCHA to challenge requests and

Issue a JavaScript challenge

Routing bot traffic.

Prevent attacks that steal sensitive data

Collect proprietary data that can lead to negative business outcomes like intellectual property theft.

Scraping

Crawl the Internet fetching data used

by search engines.

Search Engine Bots

Degrade performance and impact user experience

Impersonate identities and perform fraudulent

Credit Application Fraud

Perform money laundering via online banking

Fake Accounts

Abuse customer loyalty/reward programs.

Identify and steal gift card balances with value.

Gift Card Cracking

Identify automated script.

verify they are not from an automated script

automated attacks that use bots.

Extend defenses

restricted files or data using non-compliant searches

Restricted File Access

Determine if an HTTP request is coming from a search engine bot or customer, a search engine bot part that could improve SEO, or is this bot part

of an automated credential stuffing attack that may lead to account takeover, attacker arsenals. The question becomes intent – is this a human and potential

intelligence and customer engagement. Bots also reduce costs and scale

Bots reduce costs for basic and repetitive tasks and can improve business

Detecting Bot Attacks

Malicious Bots

Benign bots can benefit the business. Bad bots can break the business.

Detect human behavior, credit application fraud, impersonate identities and perform fraudulent transactions that could result in chargeback losses.

Leverage stolen credentials to automate large scale account takeover.

Collect and propagate information.

Leverage aggregators as a backdoor into other products, services, or company names referenced herein may be trademarks of their respective

For more information about how proactive, multi-layered bot protection can

provide human-like service through text or voice to responses.

Chatbots

Prevent excessive cloud charges

Prevent attacks that steal sensitive data

Protect current and potential customers:

Know the logic to Human Behavior:

Machine Learning (ML)

Adapt countermeasures while maintaining full efficacy

Identify and subtract points to a risk score. Then decide when and what type of action you

Assign risk scores to sessions with similar attack profiles and risk surfaces

Detect and block malicious bots without

human behavior.

uses bots and automation to imitate

Mitigate sophisticated fraud that

are increasingly being targeted by bots and

Protect mobile applications and APIs that

Be first to market but not first to breached:

Leverage stolen credentials to automate

Credential Stuffing

Identify

looks for suspicious behavior

Reverse Domain Name System lookup

Use CAPTCHA to challenge requests and

Issue a JavaScript challenge

Routing bot traffic.

Prevent attacks that steal sensitive data

Collect proprietary data that can lead to negative business outcomes like intellectual property theft.

Scraping

Crawl the Internet fetching data used

by search engines.

Search Engine Bots

Degrade performance and impact user experience

Impersonate identities and perform fraudulent

Credit Application Fraud

Perform money laundering via online banking

Fake Accounts

Abuse customer loyalty/reward programs.

Identify and steal gift card balances with value.

Gift Card Cracking

Identify automated script.

verify they are not from an automated script

automated attacks that use bots.

Extend defenses

restricted files or data using non-compliant searches

Restricted File Access

Determine if an HTTP request is coming from a search engine bot or customer, a search engine bot part that could improve SEO, or is this bot part

of an automated credential stuffing attack that may lead to account takeover, attacker arsenals. The question becomes intent – is this a human and potential

intelligence and customer engagement. Bots also reduce costs and scale

Bots reduce costs for basic and repetitive tasks and can improve business

Detecting Bot Attacks

Malicious Bots

Benign bots can benefit the business. Bad bots can break the business.

Detect human behavior, credit application fraud, impersonate identities and perform fraudulent transactions that could result in chargeback losses.

Leverage stolen credentials to automate large scale account takeover.

Collect and propagate information.

Leverage aggregators as a backdoor into other products, services, or company names referenced herein may be trademarks of their respective

For more information about how proactive, multi-layered bot protection can

provide human-like service through text or voice to responses.

Chatbots

Prevent excessive cloud charges

Prevent attacks that steal sensitive data

Protect current and potential customers:

Know the logic to Human Behavior:

Machine Learning (ML)

Adapt countermeasures while maintaining full efficacy

Identify and subtract points to a risk score. Then decide when and what type of action you

Assign risk scores to sessions with similar attack profiles and risk surfaces

Detect and block malicious bots without

human behavior.

uses bots and automation to imitate

Mitigate sophisticated fraud that

are increasingly being targeted by bots and

Protect mobile applications and APIs that

Be first to market but not first to breached:

Leverage stolen credentials to automate

Credential Stuffing

Identify

looks for suspicious behavior

Reverse Domain Name System lookup

Use CAPTCHA to challenge requests and

Issue a JavaScript challenge

Routing bot traffic.

Prevent attacks that steal sensitive data

Collect proprietary data that can lead to negative business outcomes like intellectual property theft.

Scraping

Crawl the Internet fetching data used

by search engines.

Search Engine Bots

Degrade performance and impact user experience

Impersonate identities and perform fraudulent

Credit Application Fraud

Perform money laundering via online banking

Fake Accounts

Abuse customer loyalty/reward programs.

Identify and steal gift card balances with value.

Gift Card Cracking

Identify automated script.

verify they are not from an automated script

automated attacks that use bots.