

June 26, 2019

# Understanding Bots !

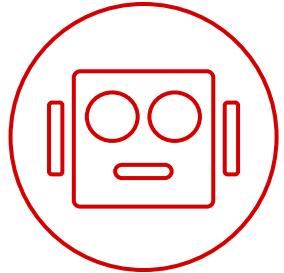
<https://github.com/shaanz/bots>

---

PRESENTED BY:

Shahnawaz Backer | Security Specialist |





## What are bots?

Why should you care?



## Common Bot Threats

Risks to apps and data



## Comprehensive App Protection

Get protection with an ROI

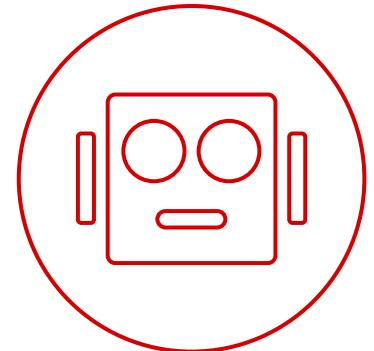
# What Is a Bot?

---

## DEFINED AS

(n) The Cambridge Dictionary

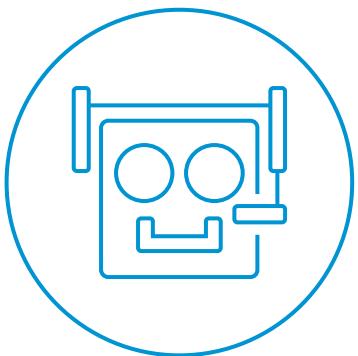
---



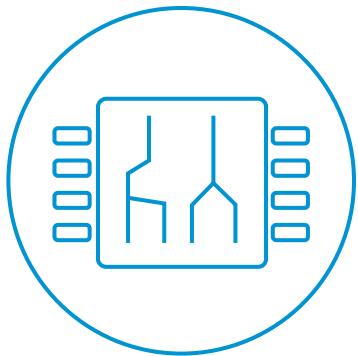
**A computer program that works automatically, especially one that searches for and finds information on the internet**

# Bots Improve User Experience

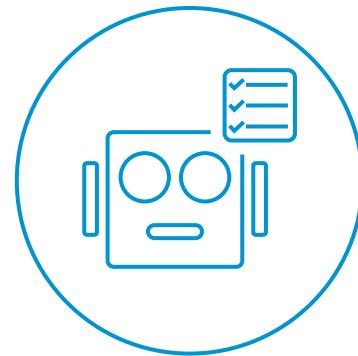
---



**Chatbot**



**Crawlers**



**Task Bot**

**"YOU EITHER DIE A HERO,**



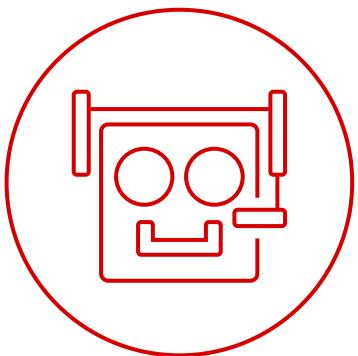
**OR LIVE LONG ENOUGH TO SEE YOURSELF  
BECOME THE VILLAIN."**

**-HARVEY DENT, THE DARK KNIGHT**

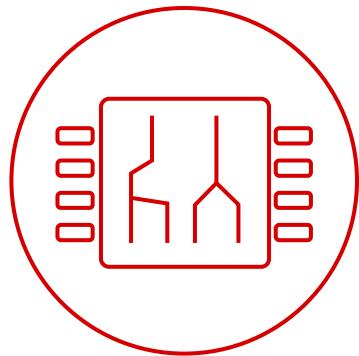


# So There Are Bad Bots

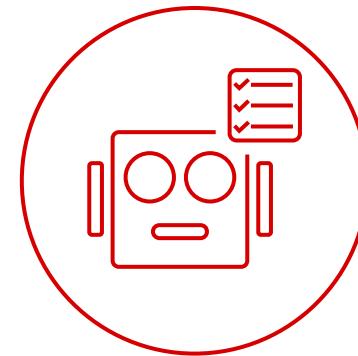
---



**Scraper Bot**



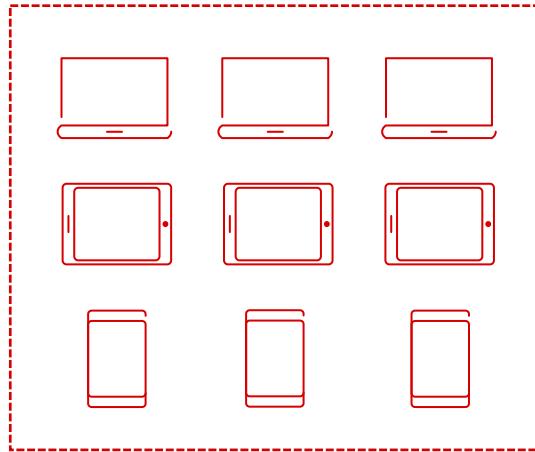
**DDoS**



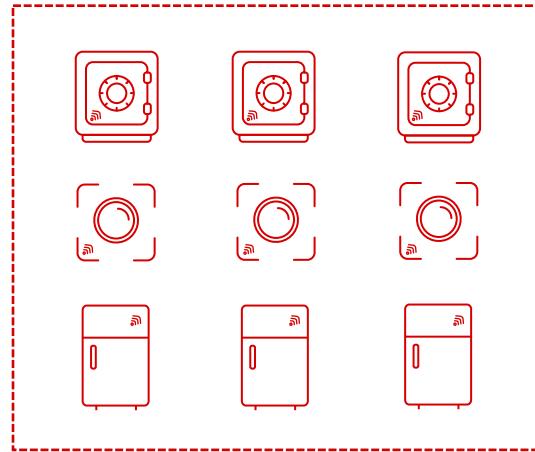
**Fraud Bots**

# What are bad bots made of?

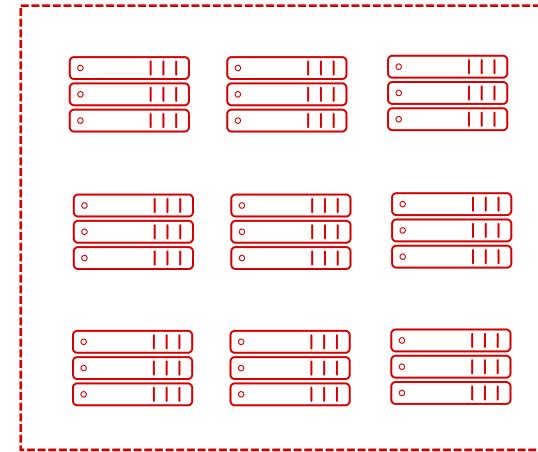
---



**Infected user  
devices**



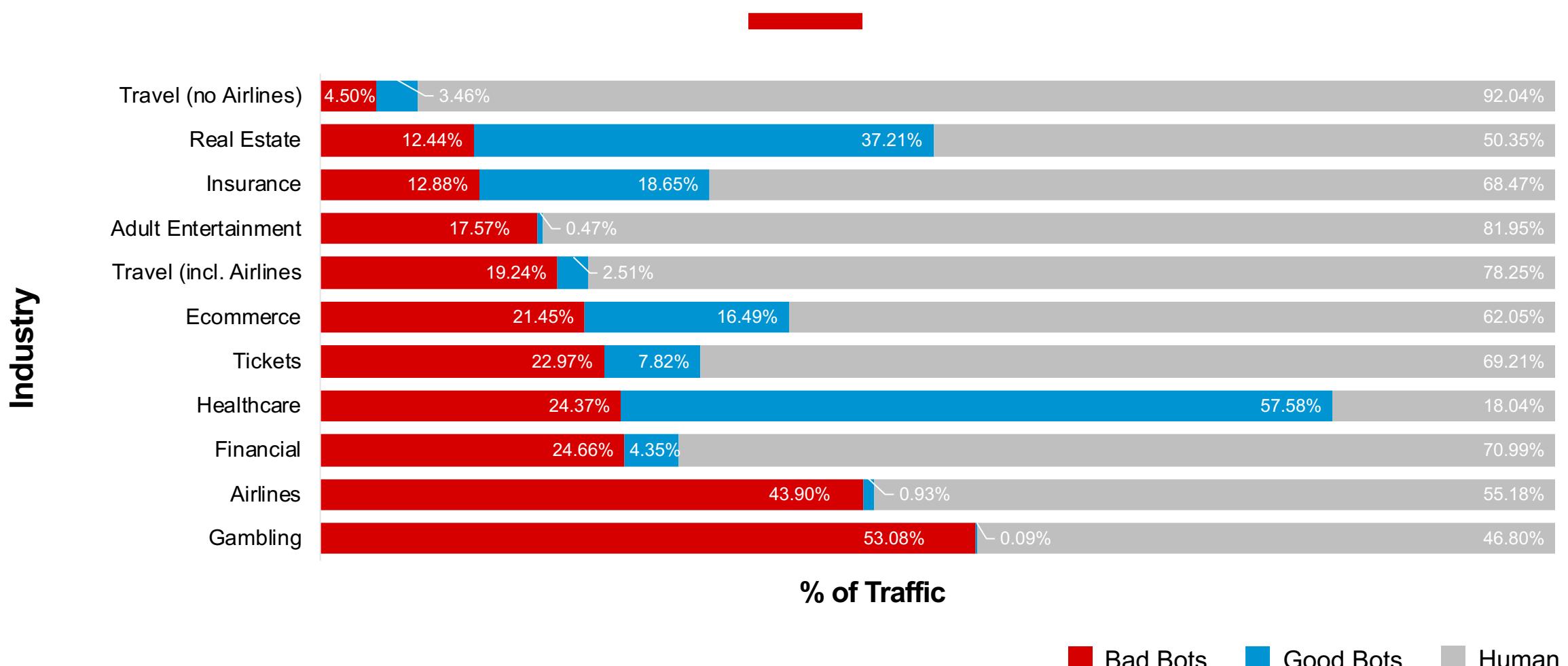
**Infected /  
compromised IoT  
devices**



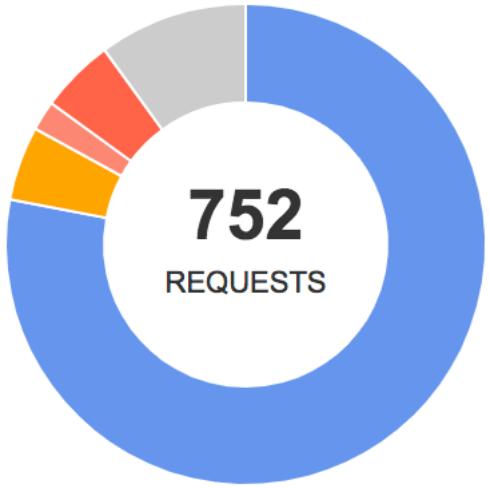
**Attacker  
owned nodes  
or processes**

# Humans vs Good Bots vs Bad Bots

## By Industry



# Put it to Test !



## Traffic by Class

■ Browser ■ Mobile Application ■ Trusted Bot ■ Untrusted Bot  
■ Suspicious Browser ■ Malicious Bot ■ Unknown

## Bot Categories

N/A	658		Suspicious Browser Types	16	
HTTP Library	38		Browser Masquerading	7	
Network Scanner	33				

# What Constitutes the Bad Bot Traffic

[← Back to vs\\_CTF](#)

Order by Incidents Count ▾ Descending ▾



Applied Fi

## Detected Bots

«

**Undefined**

Unknown

**50**  
INCIDENTS

**zgrab**

Malicious Bot (Network Scanner)

**32**  
INCIDENTS

**python-requests**

Untrusted Bot (HTTP Library)

**29**  
INCIDENTS

**Presenting as Chrome**

Suspicious Browser (Suspicious Browser Types)

**16**  
INCIDENTS

**Mozilla**

Unknown

**10**  
INCIDENTS

**Non-browser presenting as Chrome**

Malicious Bot (Browser Masquerading)

**7**  
INCIDENTS

**curl**

Untrusted Bot (HTTP Library)

**5**  
INCIDENTS

<b>Go</b>	<b>2</b>
Unknown	INCIDENTS
<b>Z</b>	<b>1</b>
Unknown	INCIDENT

# Where did it come from

**zgrab**  
Malicious Bot (Network Scanner) !

**32 INCIDENTS**

**Top Source IP Addresses** 32▼

**32 Incidents (33 Requests)**

**Time Range** ▼

2019-03-14 01:42:02 - 2019-03-14 01:42:02

2019-03-12 00:01:32 - 2019-03-12 00:01:32

2019-03-11 00:58:13 - 2019-03-11 00:58:13

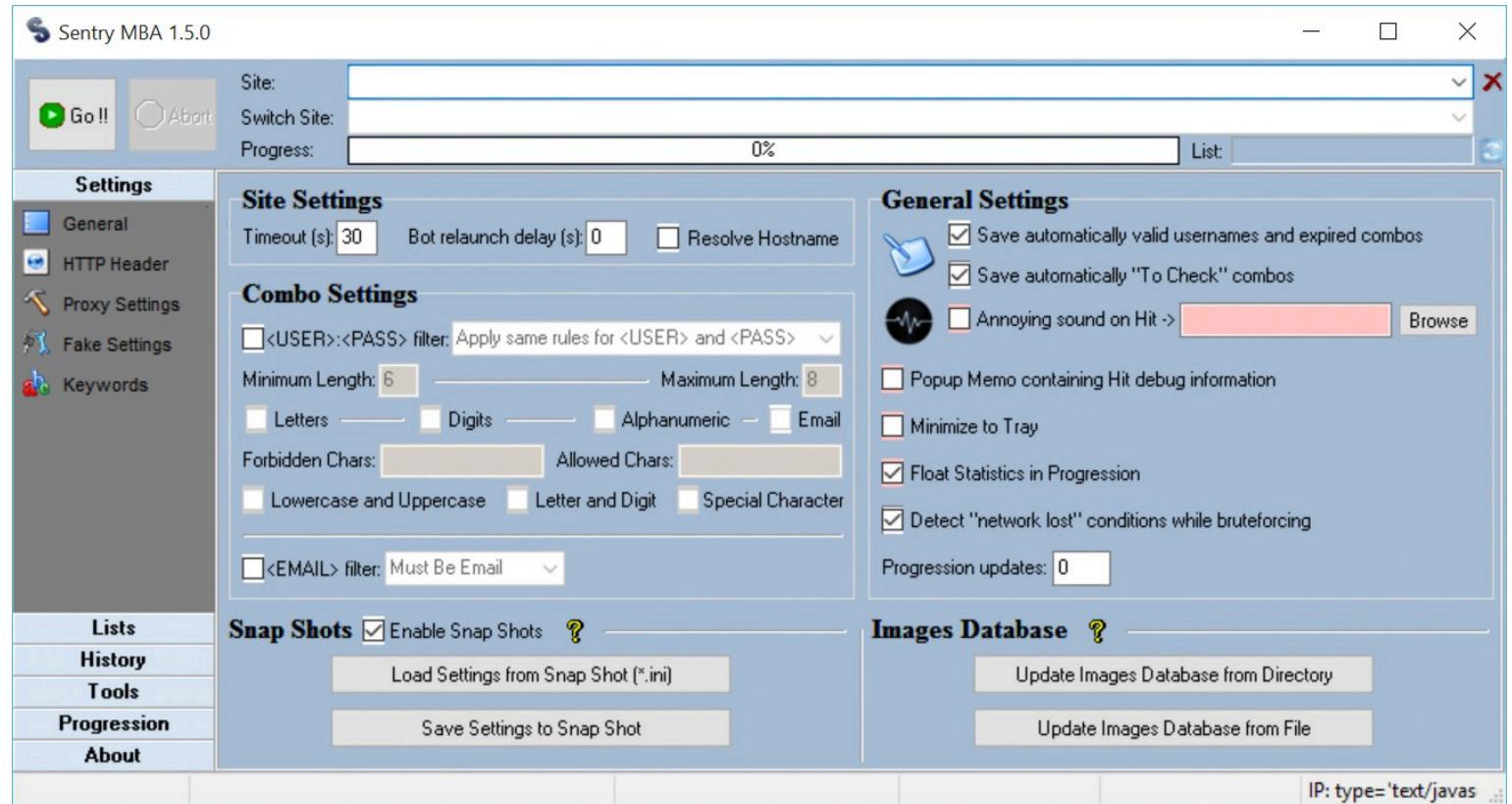
2019-03-08 13:37:13 - 2019-03-08 13:37:13

2019-03-08 00:46:28 - 2019-03-08 00:46:28

2019-03-05 00:44:08 - 2019-03-05 00:44:08

Source IP Address	
40.70.213.111	<input checked="" type="checkbox"/> [HTTPS] / zgrab (Malicious Bot) 198.108.66.128 14:08:06 2019-03-25
128.199.88.135	<input type="checkbox"/> [HTTPS] / Undefined (Unknown) 74.82.47.5 01:25:34 2019-03-25
107.170.193.203	<input type="checkbox"/> [HTTPS] / zgrab (Malicious Bot) 128.199.88.135 01:10:49 2019-03-24
89.31.100.164	<input type="checkbox"/> [HTTPS] / FireFox (Browser) 60.191.38.77 00:09:37 2019-03-24
198.108.66.48	<input type="checkbox"/> [HTTPS] / Undefined (Unknown) 216.218.206.68 23:51:07 2019-03-23
37.233.77.228	<input type="checkbox"/> [HTTPS] / zgrab (Malicious Bot) 107.170.193.203 05:15:10 2019-03-23
107.170.199.51	<input type="checkbox"/> [HTTPS] / zgrab (Malicious Bot) 107.170.193.203 05:15:10 2019-03-23

# What does bot management look like?



# C&C Management Panels

The image displays a collection of screenshots from different C&C management panels, illustrating various features and data presented to operators.

- Top Left:** A dashboard showing "Total Bots" (677), "ACCOUNTS RECEIVED" (0), and "BANKS IN PANEL" (10). It includes a chart showing 0% received and a network icon.
- Middle Left:** A table titled "Jabber Usage" listing four entries (IT\_INTES, IT\_POPSO, IT\_GBW) with columns for BN, AR, CR, Efficiency, Command, Param1, Param2, Jabber Usage (with dropdowns for OFF, ON, AI, and fwow@), and Href (links to external websites).
- Bottom Left:** A terminal window showing server\_time: 15:25:01-27.12.17 and all/active: 6928/82. Buttons include "Select Account", "Socks list", and "Add/Edit Accs".
- Bottom Left Table:** A table with columns: id, ip, firstknock, lastknock, server ip, server port, connected, auth ip, auth login, auth pass, and country. Rows show data for various IP addresses and ports.
- Top Right:** A browser-based interface titled "Tables" showing a "Manage records" table with columns: grabber, viewed, href, complete, and status. It lists multiple rows of data with details like href values such as "/2012harley", "romans523", and "1312871278...", and status codes like "complete" and "viewed".
- Middle Right:** A dashboard titled "Dashboard" with sections for "Manage records" and "Accounts". The "Accounts" section shows a table with columns: Folder, Bank, Report Time, Grabber Finished, IP Address, Bot ID, Login Details, and Balances. It includes a row for a Wells Fargo account with details like login: brandy\_dean, password: 2du0@2Dy, and balance information.
- Bottom Right:** A "Reports" section showing a table of log entries with columns: Report Date/Time, Message Type, Browser, Return Function, and Message. The messages describe the抓取器 (grabber) finishing its task, the holder logging in, and the card fake being submitted.

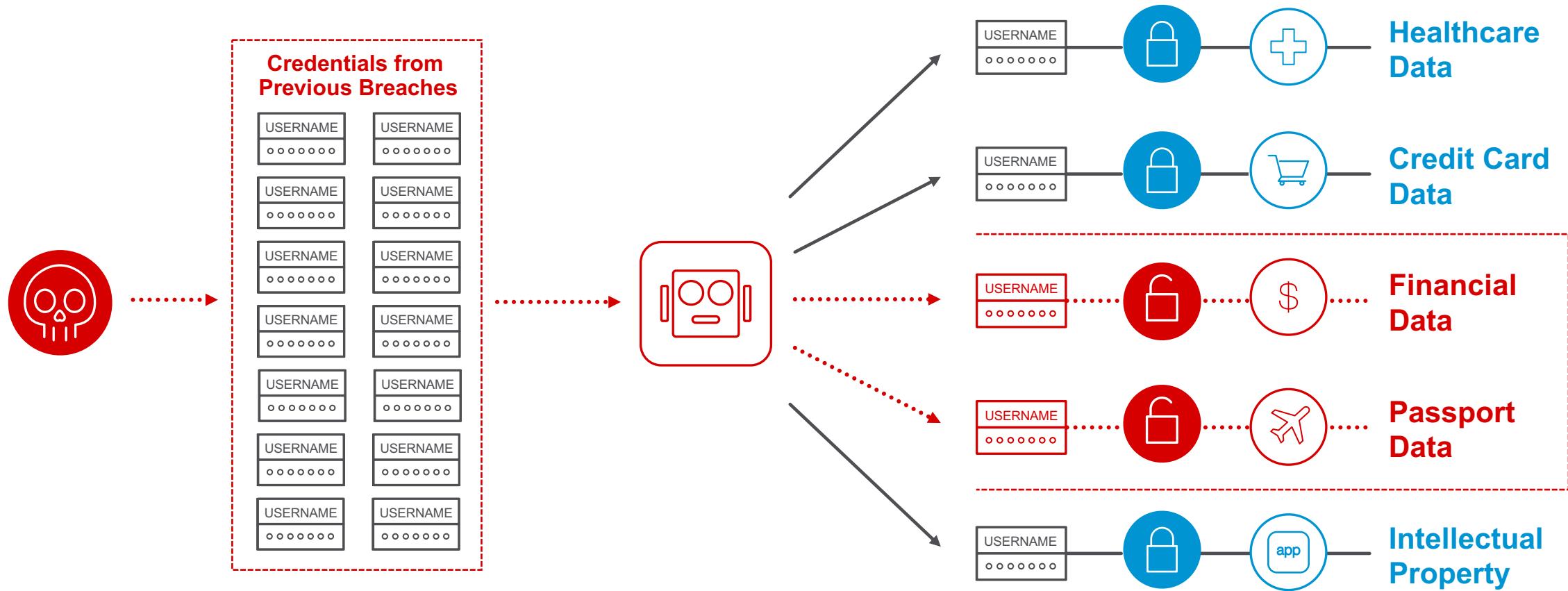
# Attack Vector



# How do bots attack the app layer?

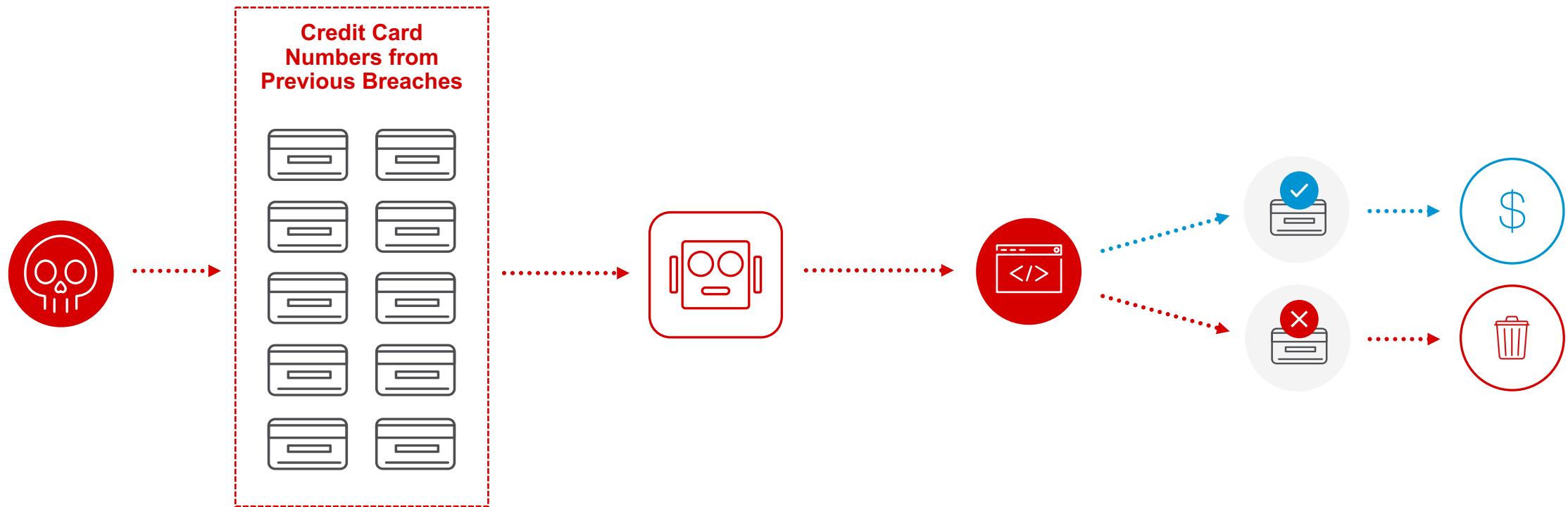
Threat Category	Attack Name	Description
Account Takeover	Credential Stuffing	Mass log in attempts used to verify the validity of stolen username/password pairs.
	Credential Cracking	Identify valid login credentials by trying different values for usernames and/or passwords.
	Account Aggregation	Used by an intermediary application that collects together multiple accounts and interacts on their behalf.
	Account Creation	Create multiple accounts for subsequent misuse.
Payment Card Data	Carding	Multiple payment authorisation attempts used to verify the validity of bulk stolen payment card data.
	Card Cracking	Identify missing start/expiry dates and security codes for stolen payment card data by trying different values.
	Cashing Out	Buy goods or obtain cash utilising validated stolen payment card or other user account data.
Vulnerability Scanning	Footprinting	Probe and explore application to identify its constituents and properties.
	Vulnerability Scanning	Crawl and fuzz application to identify weaknesses and possible vulnerabilities.
	Fingerprinting	Elicit information about the supporting software and framework types and versions.
Denial of Service / Resource Hoarding	Scalping	Obtain limited-availability and/or preferred goods/services by unfair methods.
	Denial of Inventory	Deplete goods or services stock without ever completing the purchase or committing to the transaction.
	Denial of Service (DoS)	Target resources of the application and database servers, or individual user accounts, to achieve denial of service (DoS).
	Sniping	Last minute bid or offer for goods or services.
	Expediting	Perform actions to hasten progress of usually slow, tedious or time-consuming actions.
Content Theft	Scraping	Collect application content and/or other data for use elsewhere.
Other	Ad Fraud	False clicks and fraudulent display of web-placed advertisements.
	CAPTCHA Defeat	Solve anti-automation tests.
	Skewing	Repeated link clicks, page requests or form submissions intended to alter some metric.
	Spamming	Malicious or questionable information addition that appears in public or private content, databases or user messages.
	Token Cracking	Mass enumeration of coupon numbers, voucher codes, discount tokens, etc.

# Credential Stuffing



# Carding

---



# Vulnerability Scanning

---

Attackers must automate to find weaknesses for manual probing

---

Bots allow attackers to scale their operations

---

Many reconnaissance tools available

- Shodan, publicwww.com, BuiltWith.com, etc
- Network mappers (Nmap)
- WGET, SQLMap, etc.
- Headless browsers (Phantom.js, Selenium)

# Scalping

Supreme

heated  
sneaks

YEEZY



## Shoe Size

## Nike Account

Beta Better Nike Bot

Deactivate Tools Help Check for updates

Settings

Twitter Settings

Twitter Account: testnikebot@gmail.com

Twitter Password: .....  
 Monitor Account: nike  
 Disable Twitter (Use Only Early Links)

Options

Size Type: All Site: Nike US

Advanced Options

Use Old ATC Method  
[Link Booster](#)  
[Notification Settings](#)  
[Add/Edit Proxies](#)  
[Create Bulk Nike Accounts](#)  
[Manage Cards](#)

Reset All Settings

Accounts

Email Address	Size	Keywords	Collection Keywords	Early Links	Proxy	Checkout
bettemikebottest@gmail.com	10			https://www.nike.com/snkr/thread/badb4...		CC Checkout - Test

Add Edit Remove Clone Total Accounts: 1 Edit Account Info Edit Accounts

Start Stop View Added Products Pause Log

Test Captcha Clear Log

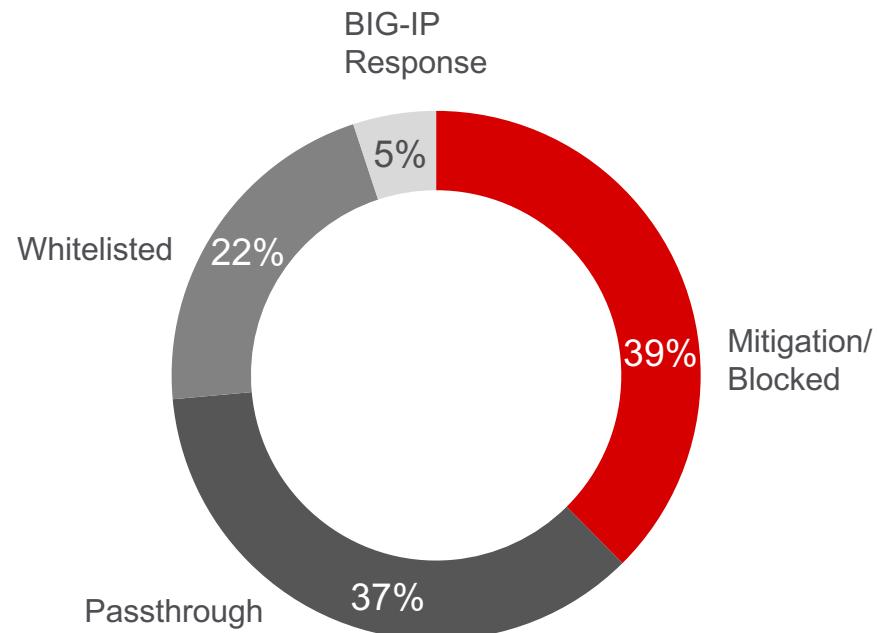
Log

```
20-Mar-17 2:10:53.4315 PM - Waiting for all accounts to log in.  
20-Mar-17 2:10:53.4746 PM - bettemikebottest@gmail.com: Logging in to Nike.  
20-Mar-17 2:10:54.5336 PM - bettemikebottest@gmail.com: Login Error! The remote server returned an error: (401) Unauthorized.  
20-Mar-17 2:10:56.2168 PM - Stopped by user.
```

# Content Scraping

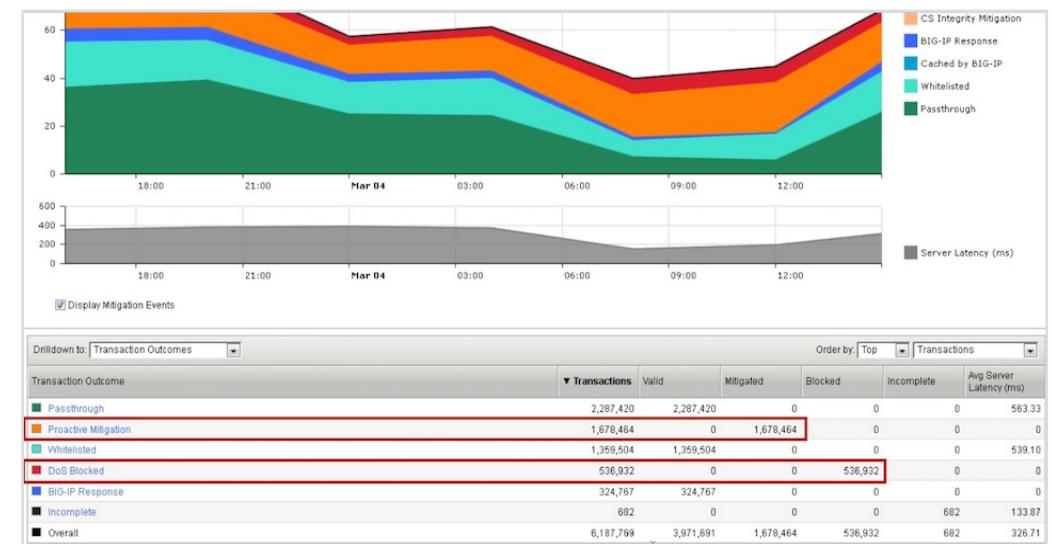
## Price Scraping

Bots monitor prices to inform competitors how they can undercut.



## Availability Tracking

Bots monitor for supply exhaustion to inform competitors of an opportunity to raise prices.

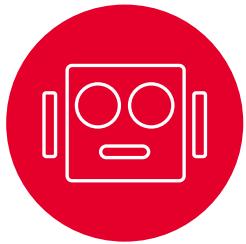


# Lessons Learned

---



# Today's Approach



## Code-level security

Difficultly differentiating between humans and modern bots

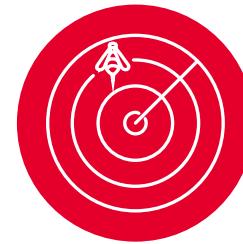
Lags behind rapid pace of bot evolution



## IP blocking

Sheer volume of IPs difficult to track and block

Ineffective at blocking TOR-based bots

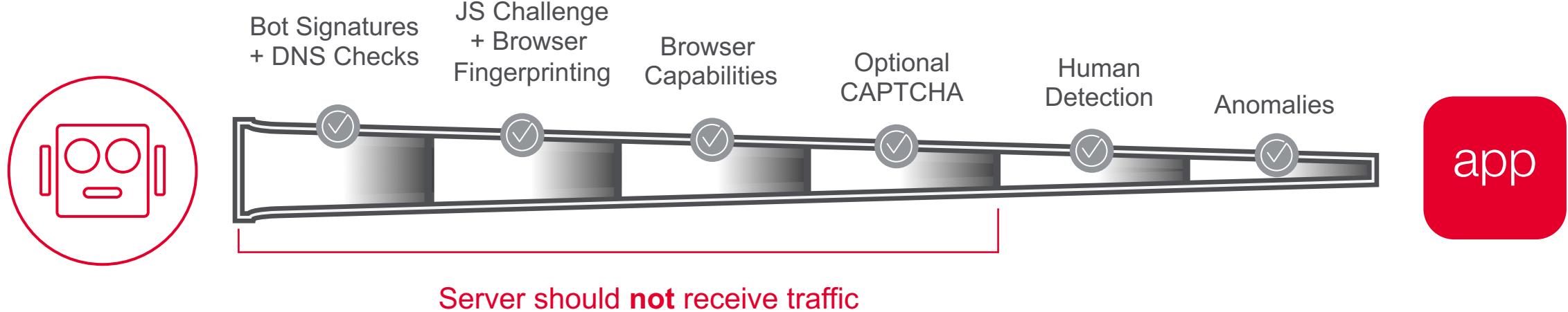


## Traditional WAF

Designed to protect against OWASP Top 10

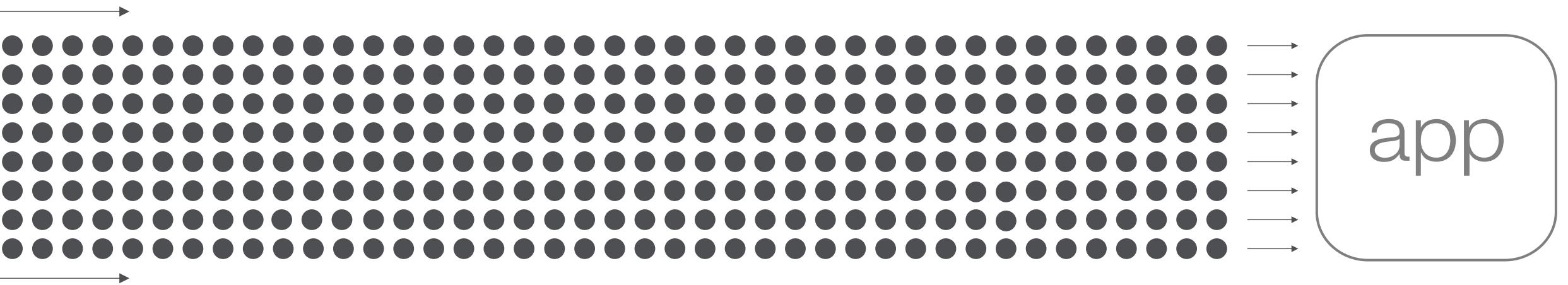
Rely solely on captcha for bot protection

# What is Required for Accurate Bot Detection?



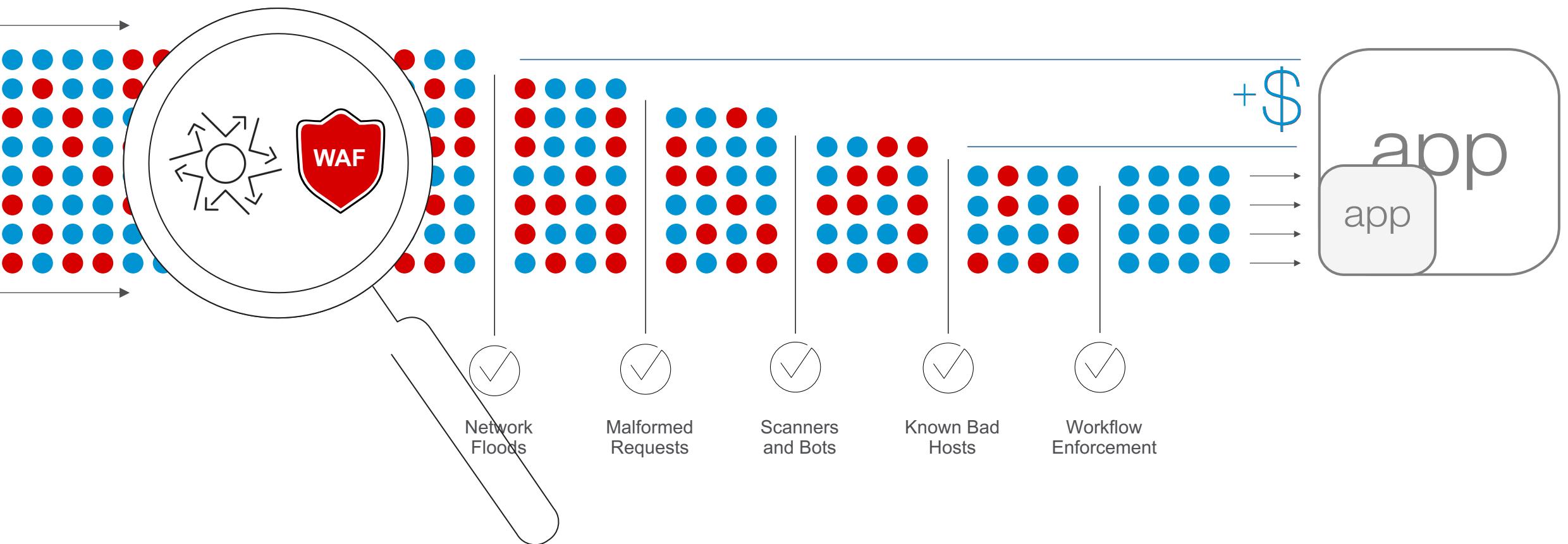
# Introducing EDoS

---



# Reduce Cloud Costs

---



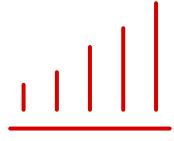
# Key Takeaways

---



Classify and control  
increasingly  
automated traffic

---



Bot detection  
requires less  
per-application tuning

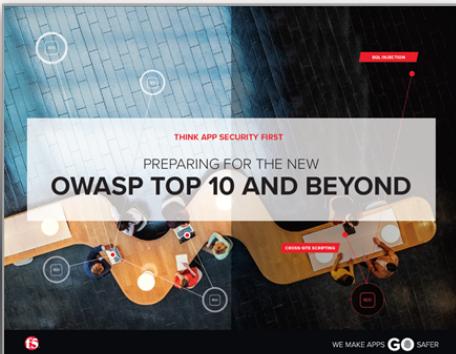
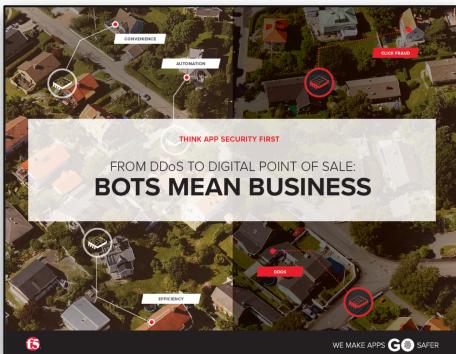
---



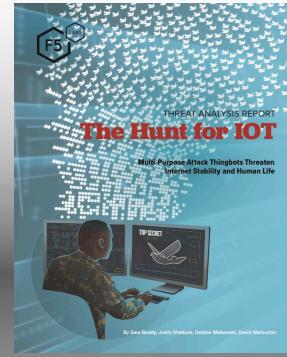
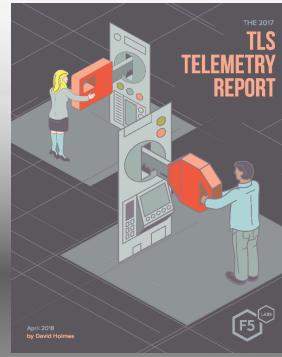
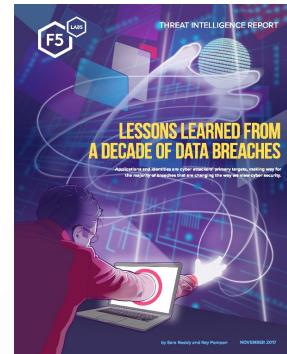
Eliminating  
30–40% of web traffic  
has a big impact

---

# Read more about these and other threats



# Stay up-to-date. Sign up for F5 Labs.



<https://interact.f5.com/AppProtectLibrary>

[F5labs.com](http://F5labs.com)

