June 26, 2019

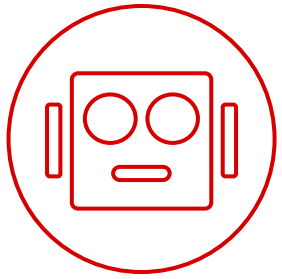
Understanding Bots !

https://github.com/shaanz/bots

PRESENTED BY:

Shahnawaz Backer | Security Specialist |

@sbacker27



What are bots?

Why should you care?

Common Bot Threats

Risks to apps and data

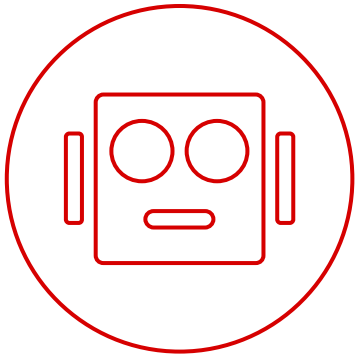
Comprehensive App Protection

Get protection with an ROI

What Is a Bot?

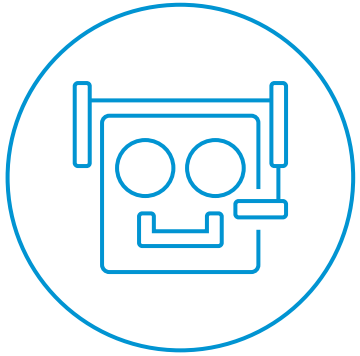
DEFINED AS

(n) The Cambridge Dictionary

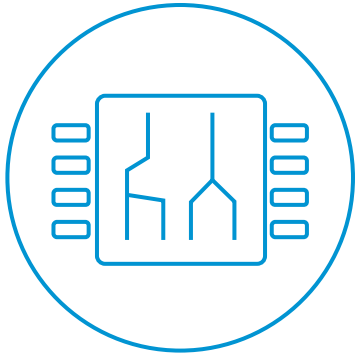


A computer program that works automatically, especially one that searches for and finds information on the internet

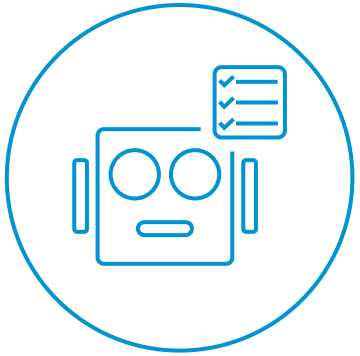
Bots Improve User Experience



Chatbot



Crawlers



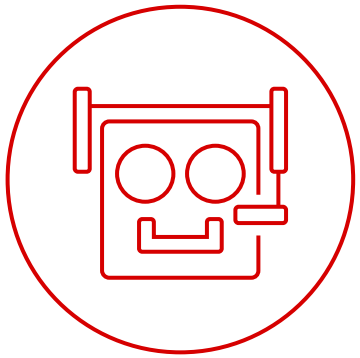
Task Bot

"YOU EITHER DIE A HERO,

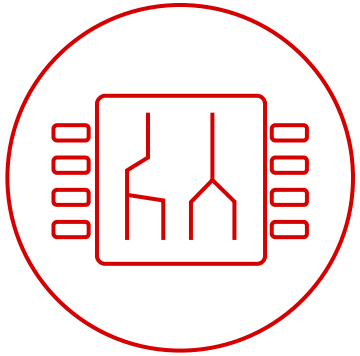
OR LIVE LONG ENOUGH TO SEE YOURSELF BECOME THE VILLAIN."

-HARVEY DENT, THE DARK KNIGHT

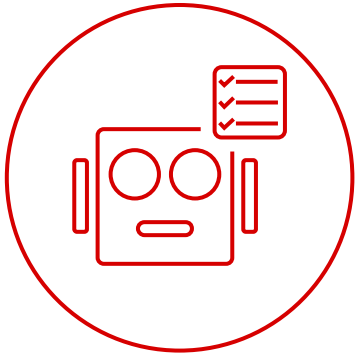
So There Are Bad Bots



Scraper Bot

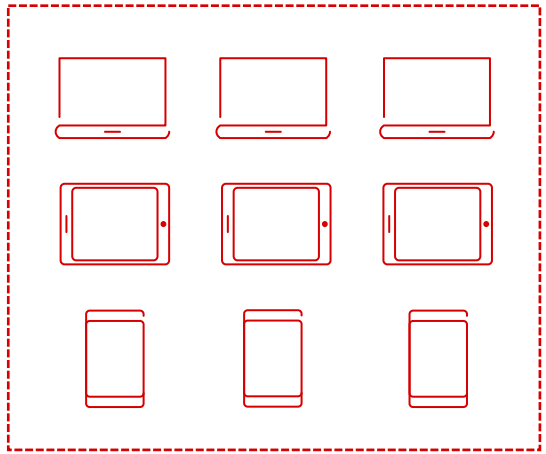


DDoS

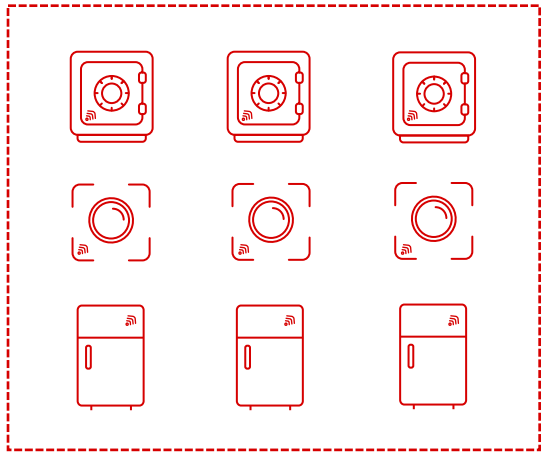


Fraud Bots

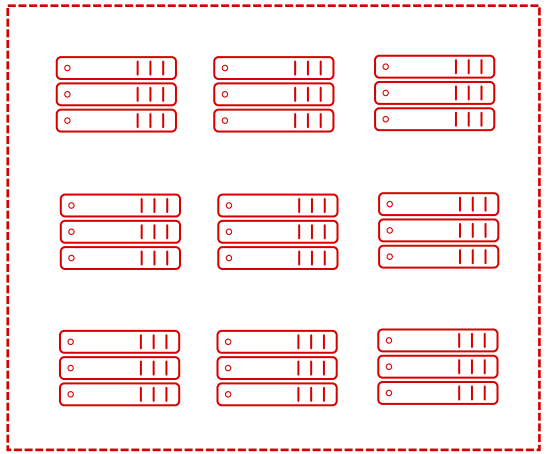
What are bad bots made of?



Infected user devices



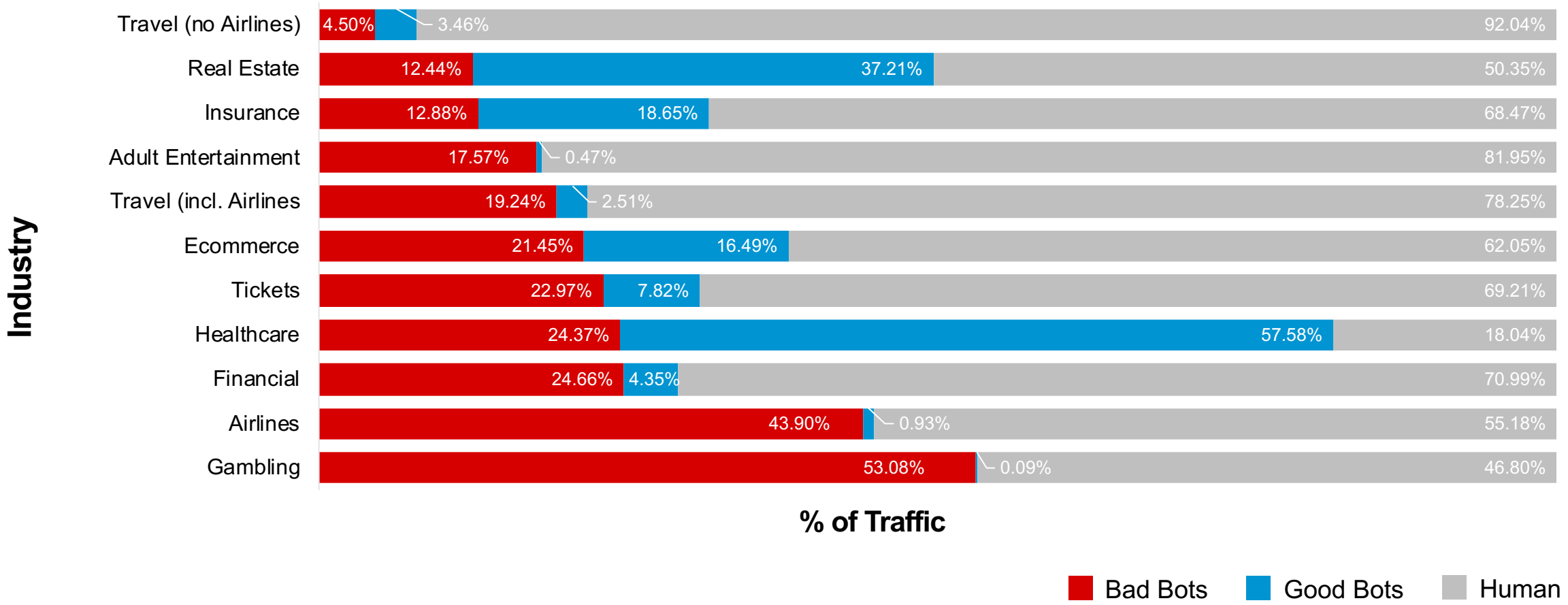
Infected / compromised IoT devices



Attacker owned nodes or processes

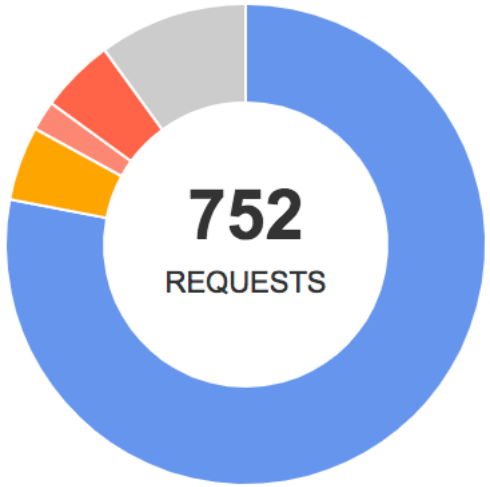
Humans vs Good Bots vs Bad Bots

By Industry



https://www.globaldots.com/2018-bad-bot-report-the-year-bad-bots-went-mainstream/

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		

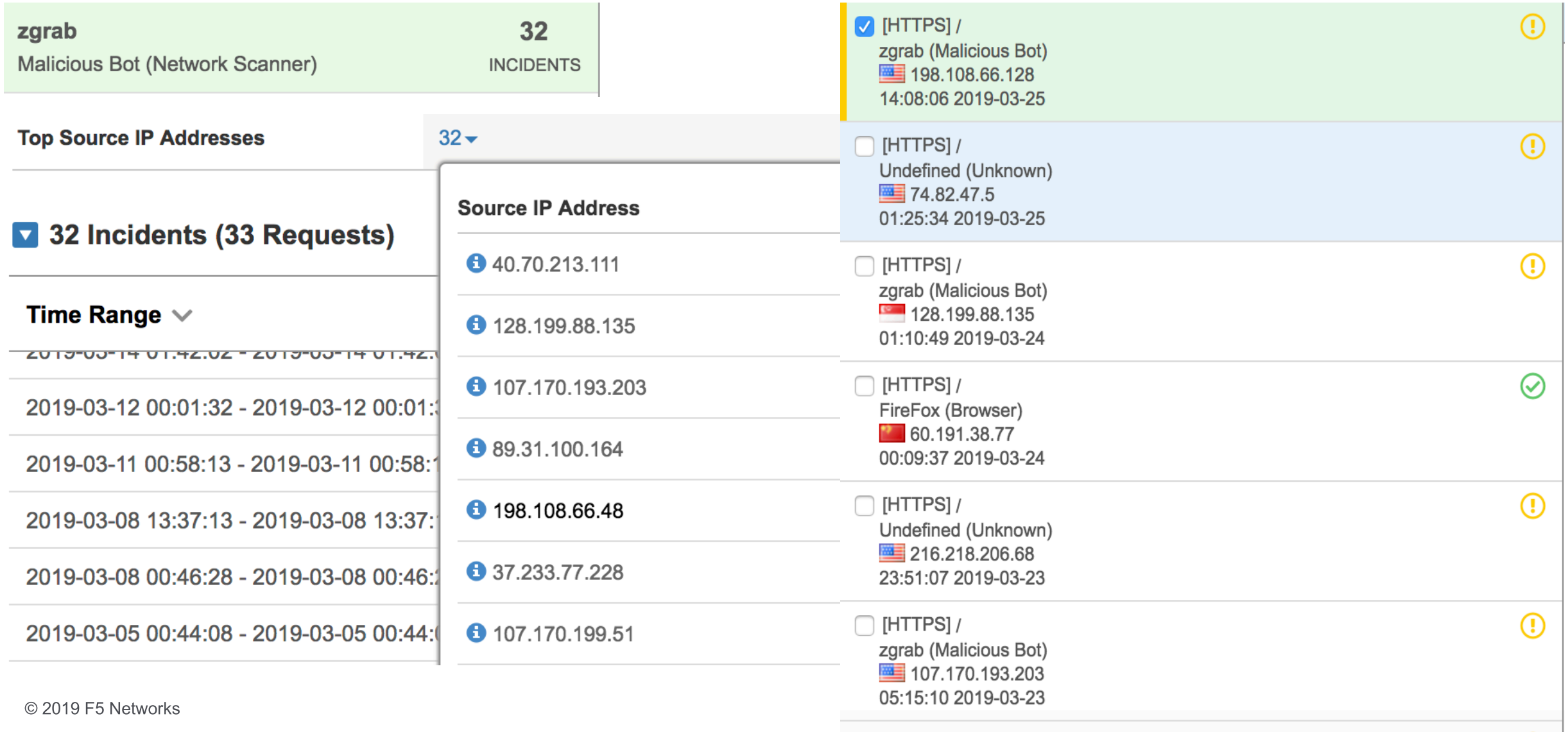
What Constitutes the Bad Bot Traffic

← Back to **vs_CTF** | Order by Incidents Count ▾ Descending ↓ | ▽ ▾ | Applied Fi

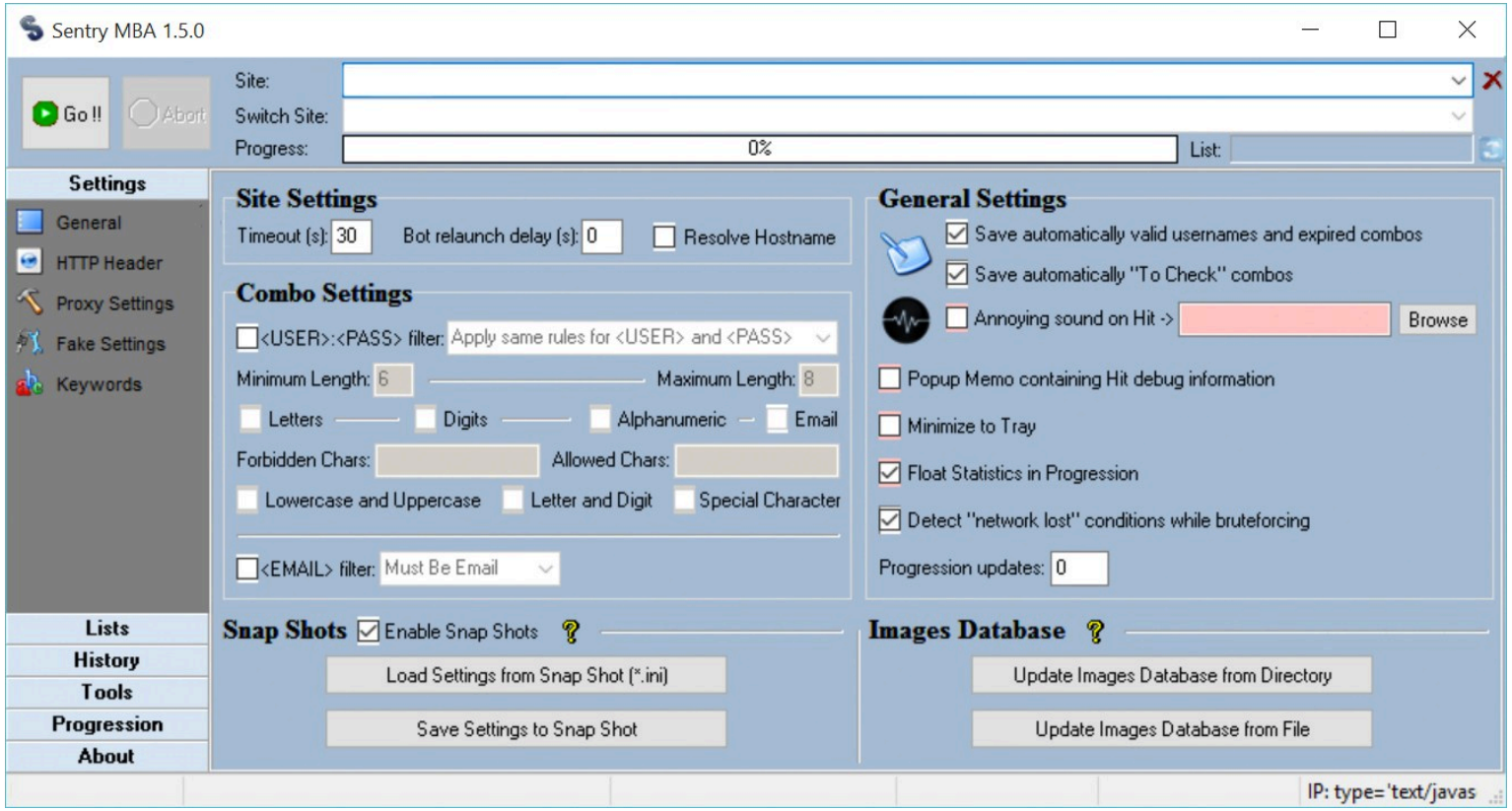
Detected Bots	«
Undefined Unknown	**50** INCIDENTS
zgrab Malicious Bot (Network Scanner)	**32** INCIDENTS
python-requests Untrusted Bot (HTTP Library)	**29** INCIDENTS
Presenting as Chrome Suspicious Browser (Suspicious Browser Types)	**16** INCIDENTS
Mozilla Unknown	**10** INCIDENTS
Non-browser presenting as Chrome Malicious Bot (Browser Masquerading)	**7** INCIDENTS
curl Untrusted Bot (HTTP Library)	**5** INCIDENTS

Go Unknown	**2** INCIDENTS
Z Unknown	**1** INCIDENT

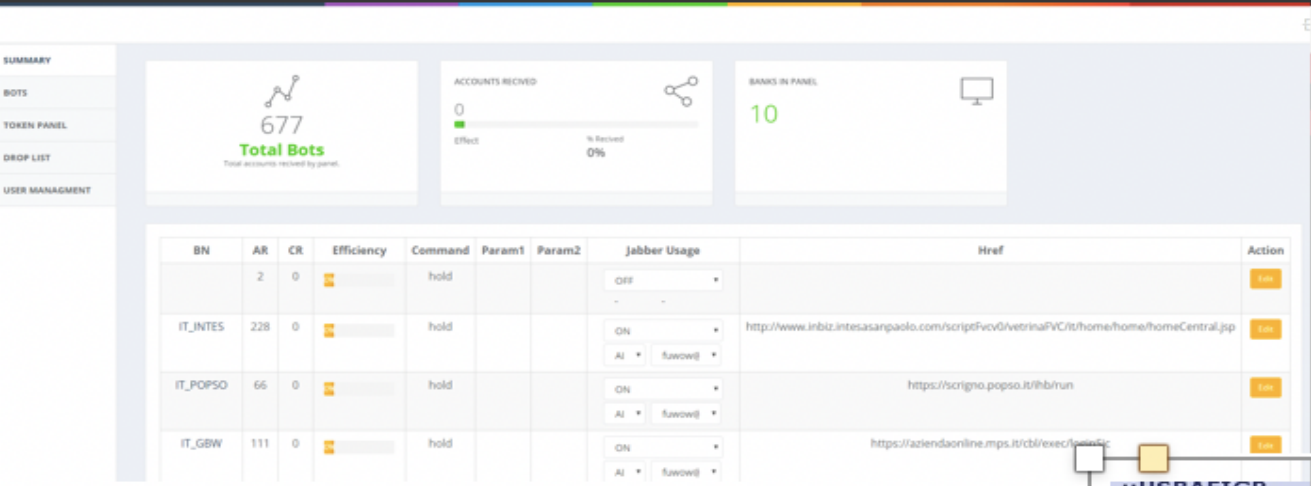
Where did it come from

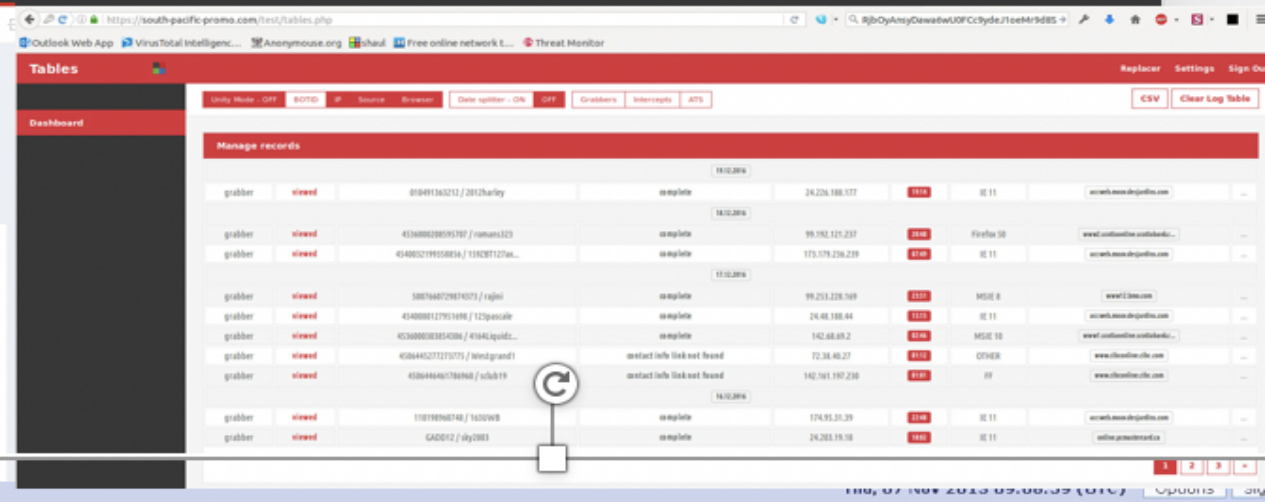


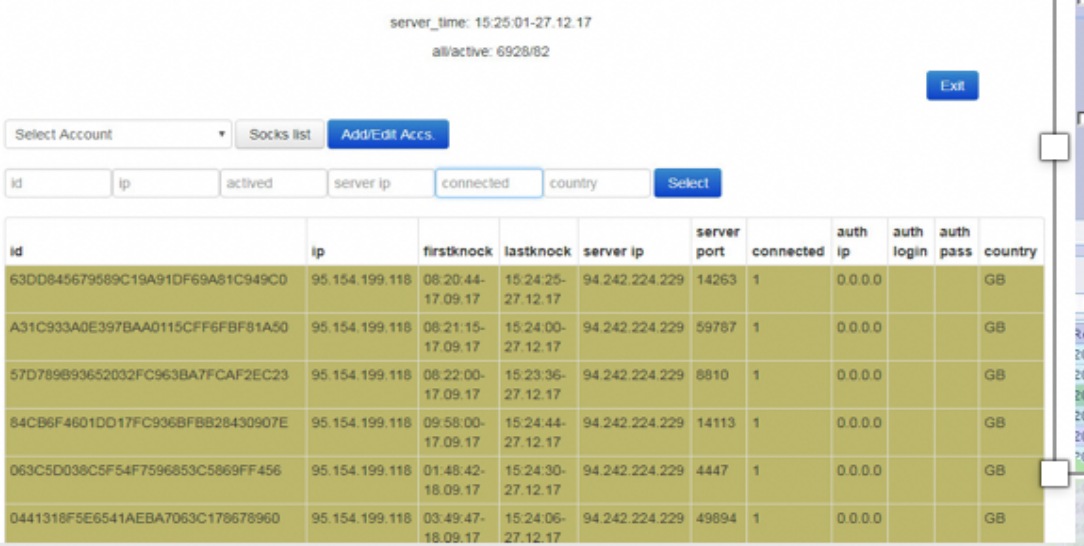
What does bot management look like?

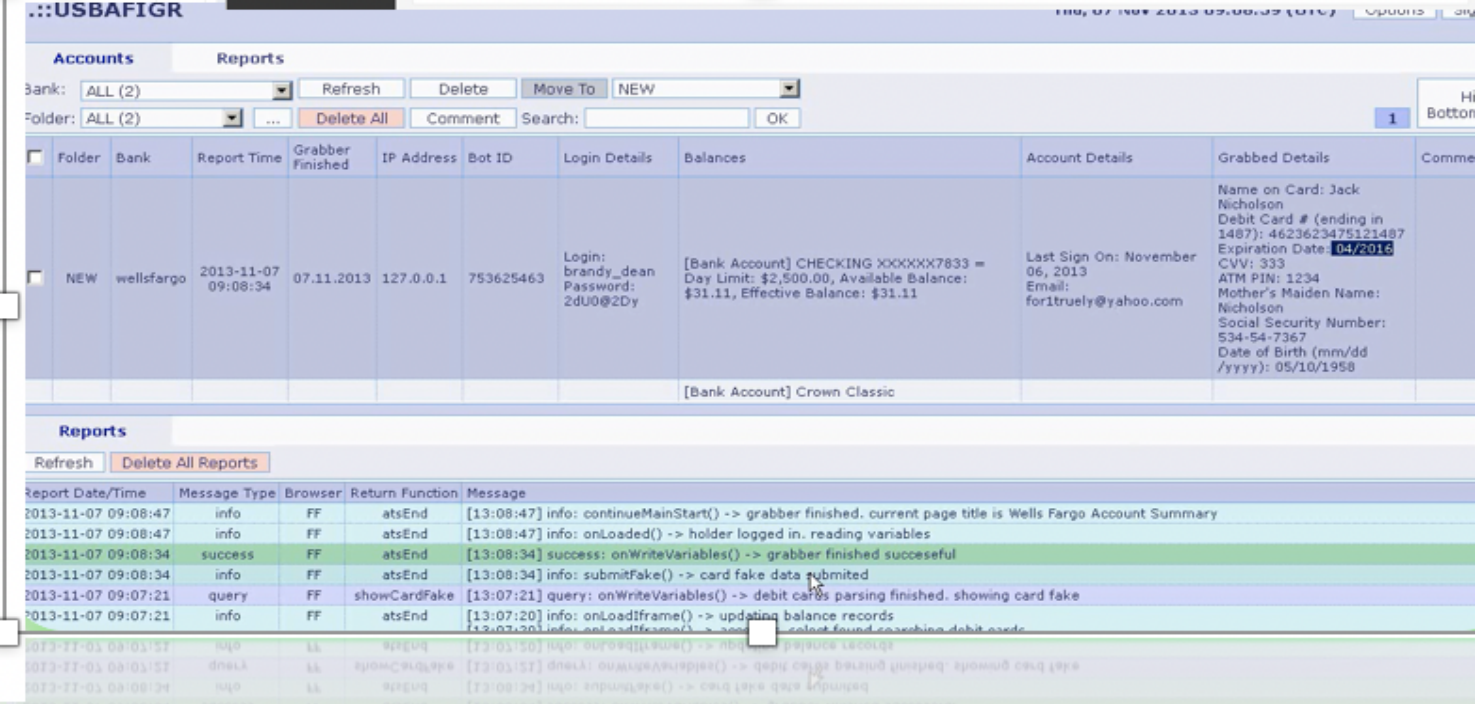


C&C Management Panels







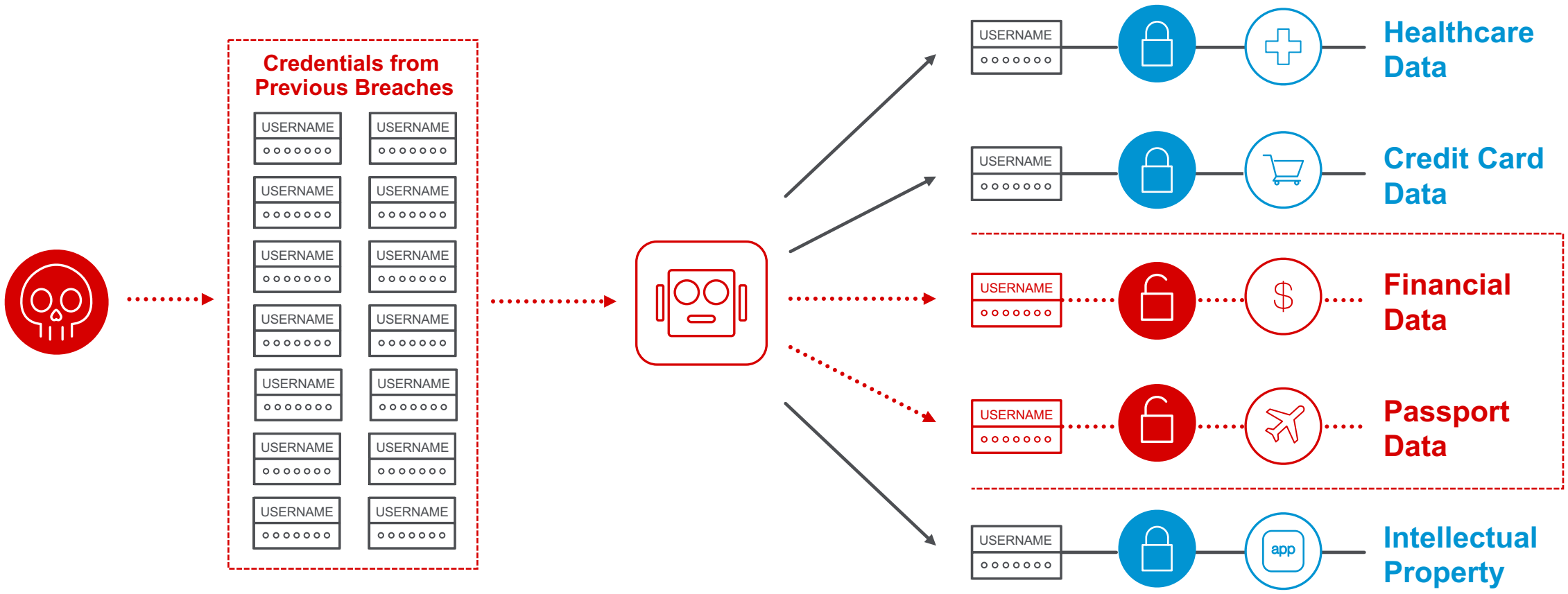


Attack Vector

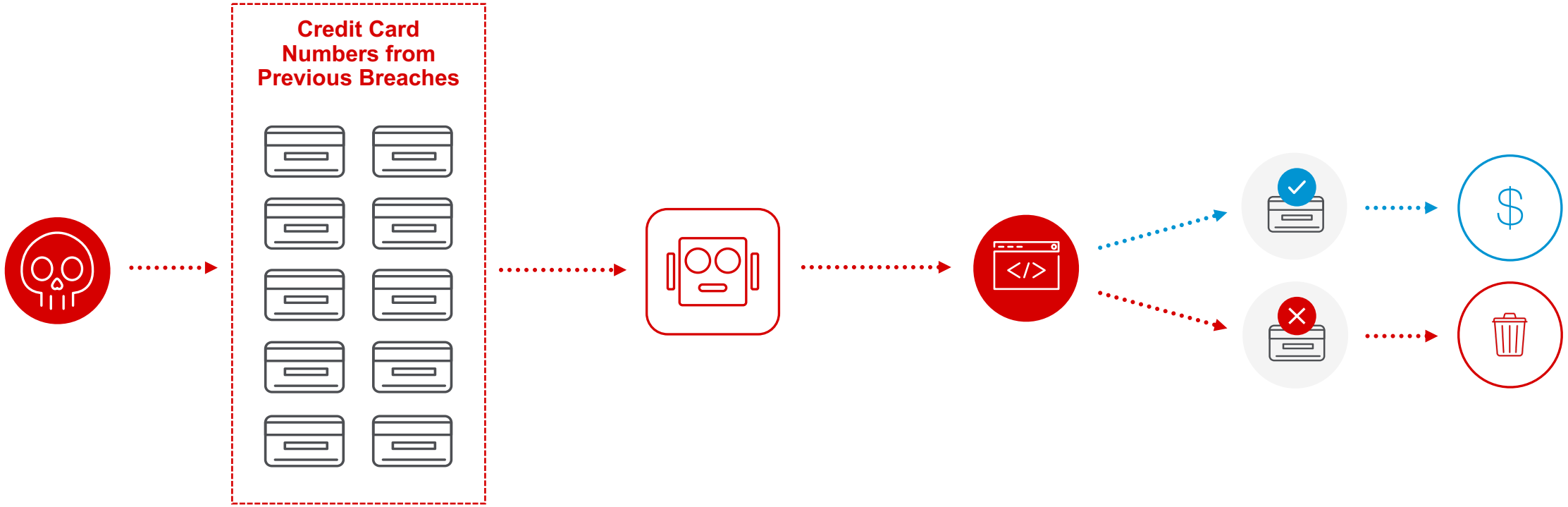
How do bots attack the app layer?

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

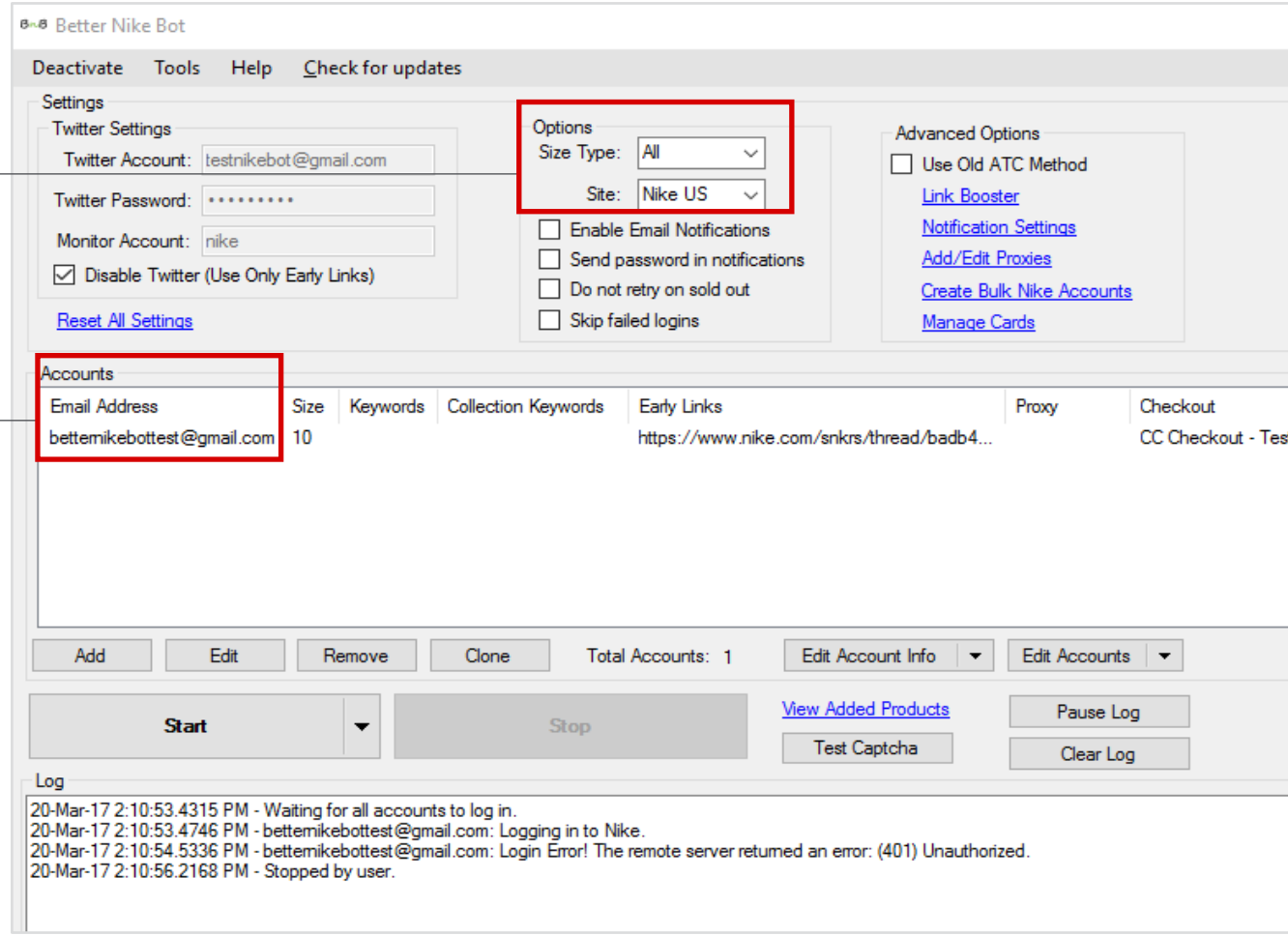
heated sneaks

YEEZY

PALACE

Shoe Size

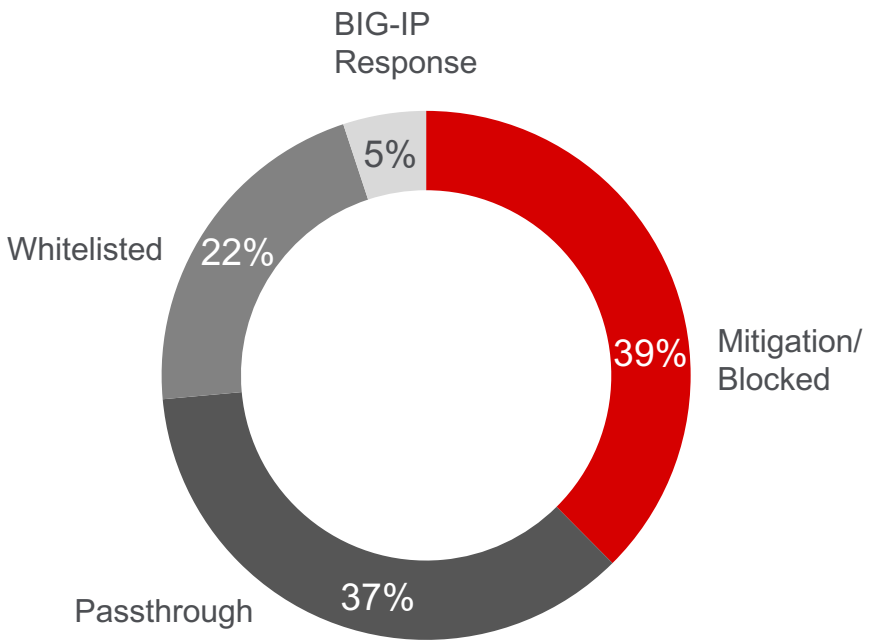
Nike Account



Content Scraping

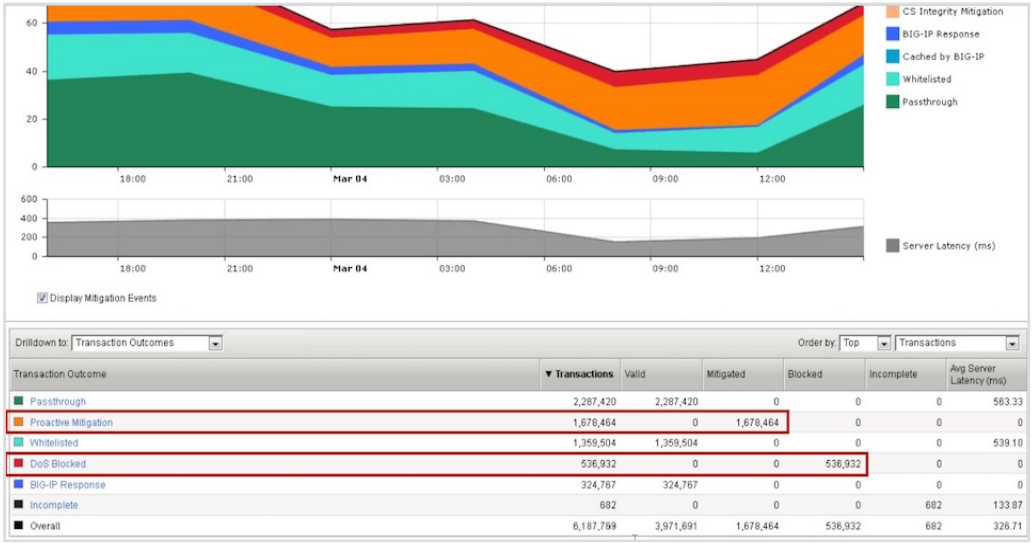
Price Scraping

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

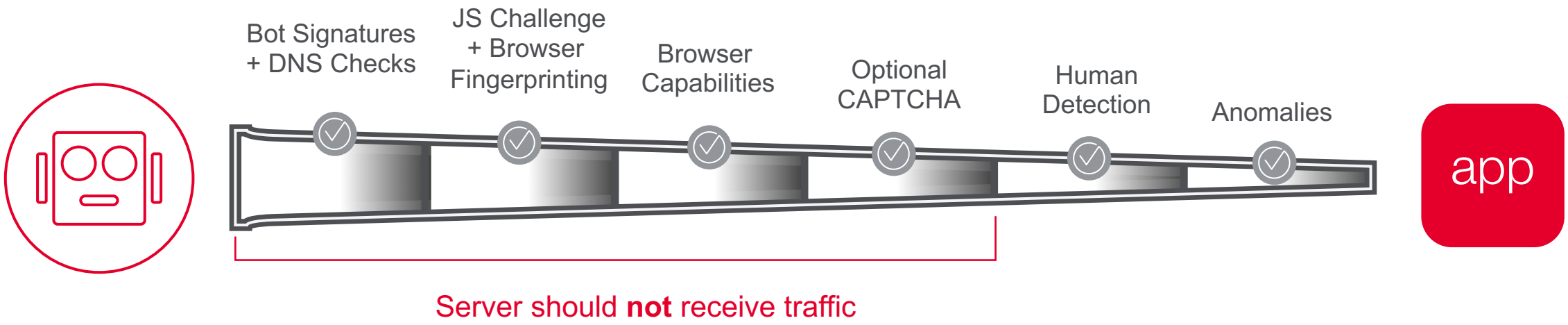
Ineffective at blocking TOR-based bots

Traditional WAF

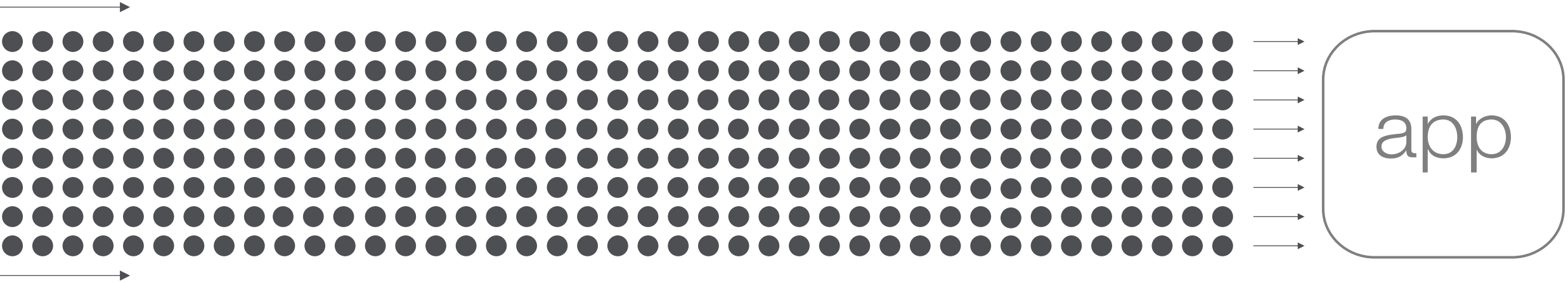
Designed to protect against OWASP Top 10

Rely solely on captcha for bot protection

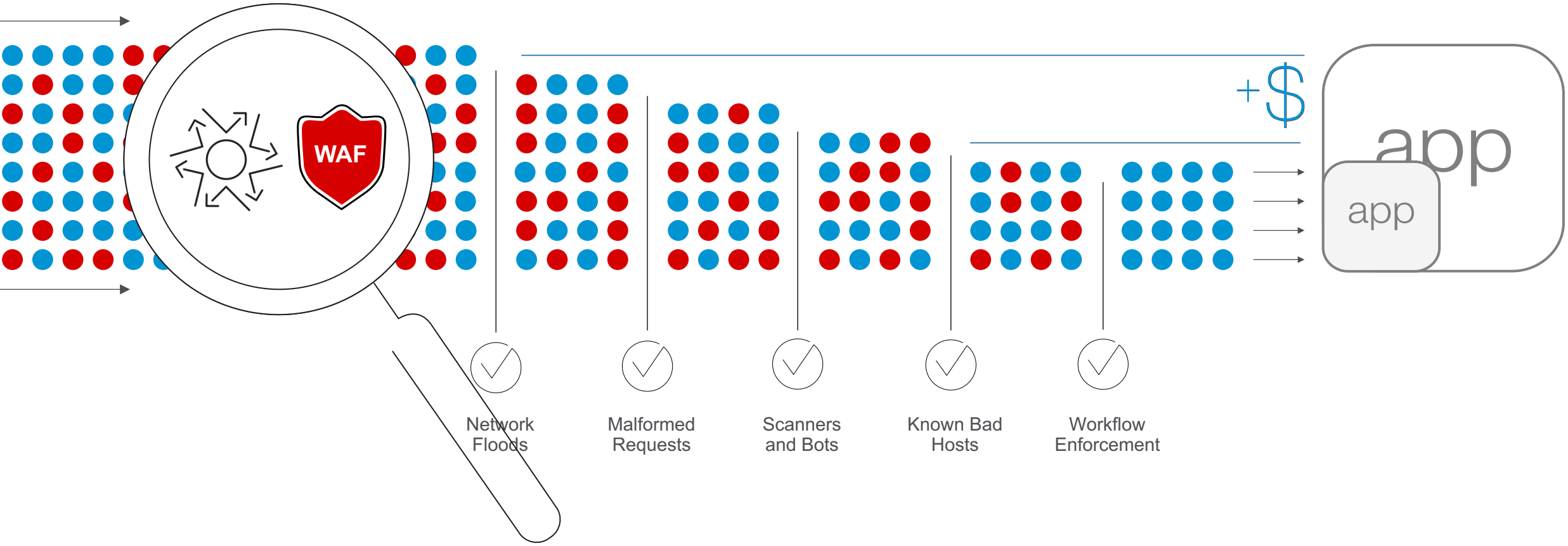
What is Required for Accurate Bot Detection?



Introducing EDoS

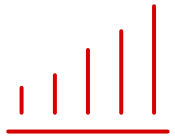


Reduce Cloud Costs



Key Takeaways

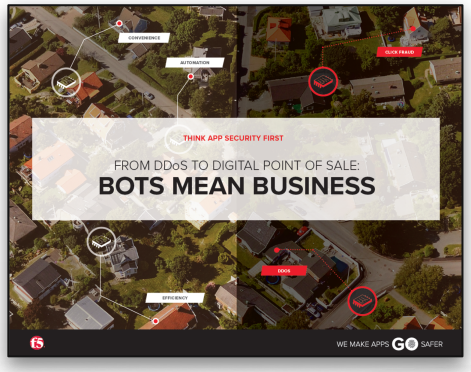
Classify and control increasingly automated traffic



Bot detection requires less per-application tuning

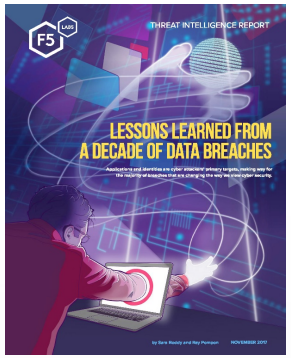
Eliminating 30–40% of web traffic has a big impact

Read more about these and other threats



https://interact.f5.com/AppProtectLibrary

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



F5labs.com