



TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT

WAF – Advanced Bot Protection

Deep Dive

Agenda

Bots & botnets – a short history

The bot problem - Industry impact

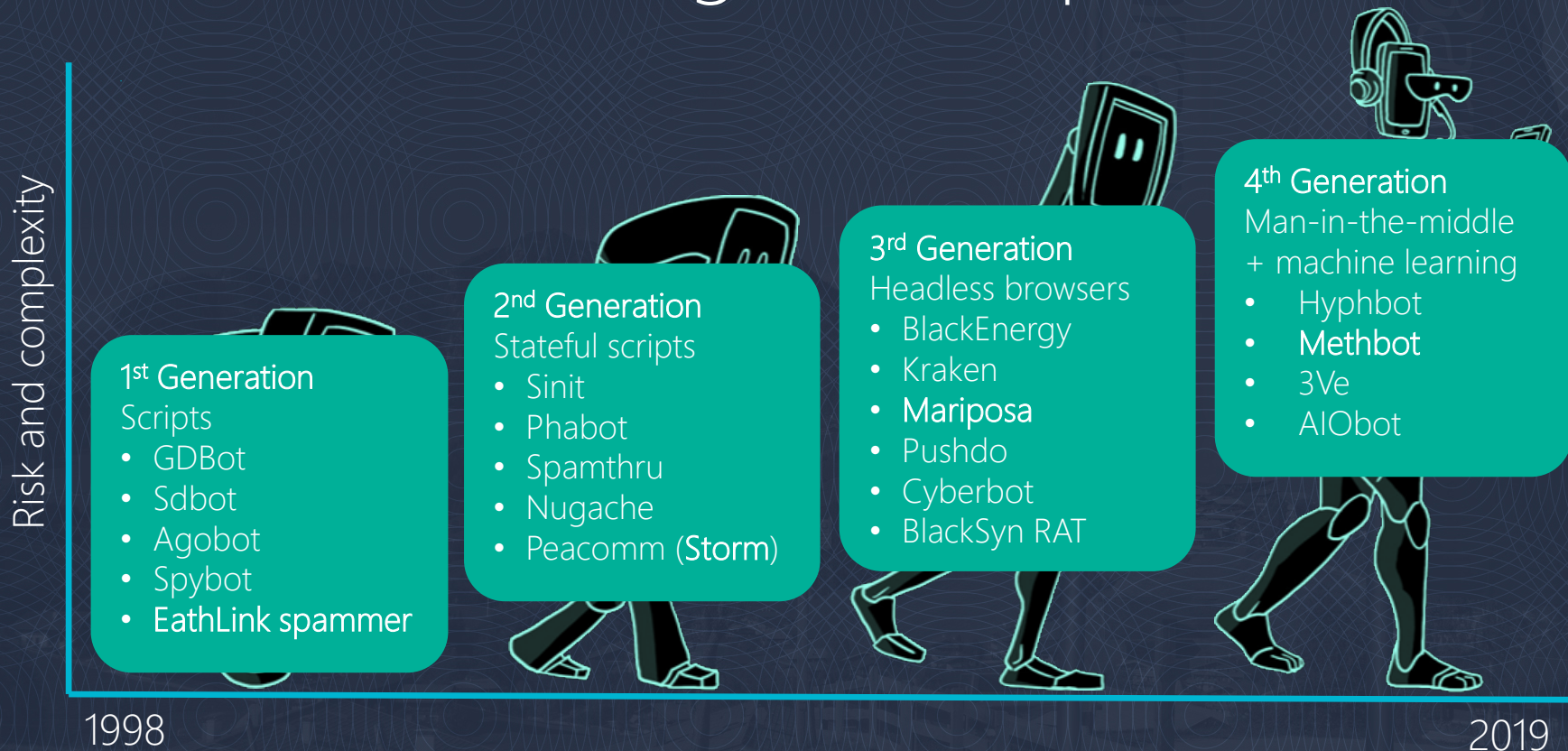
The Barracuda solution



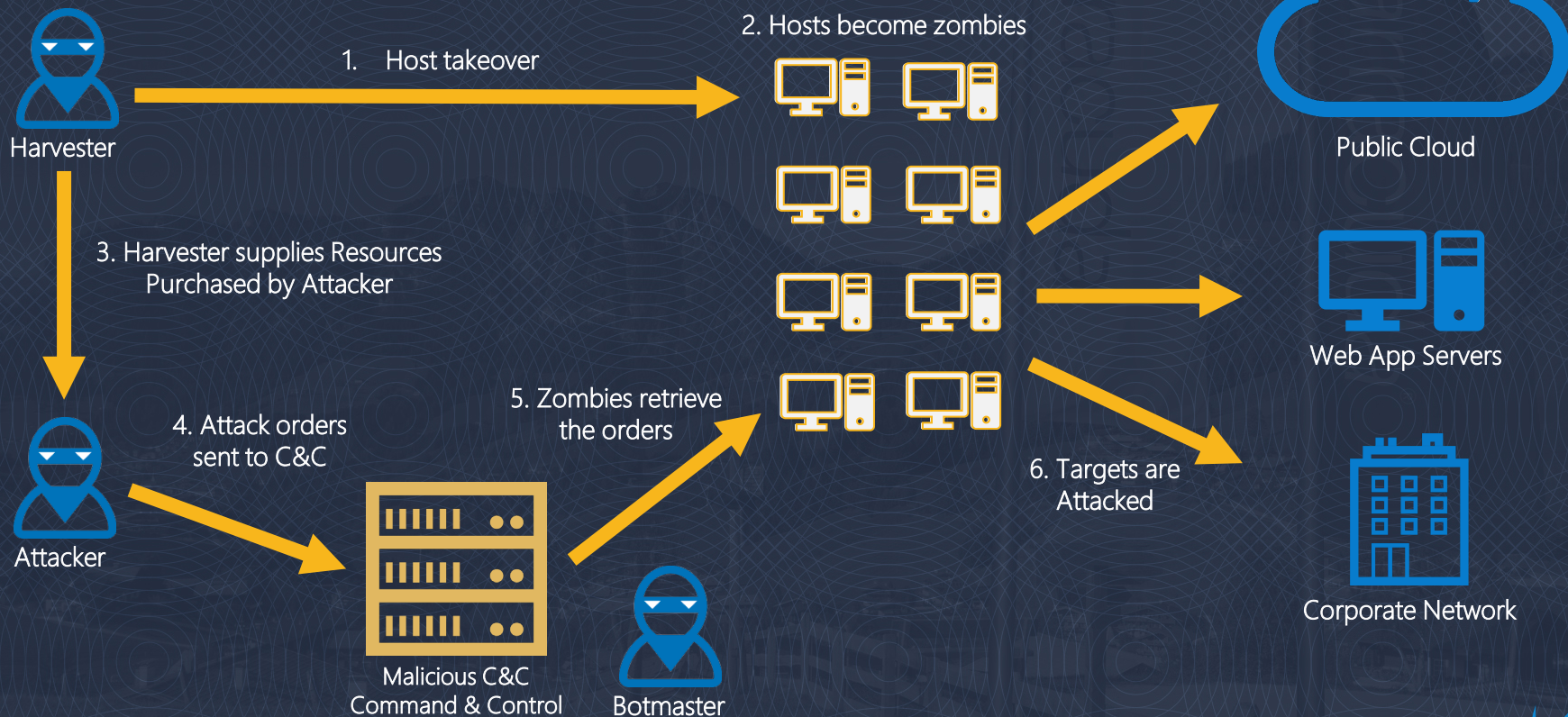
A Short history of bots



Bots are becoming more sophisticated



Anatomy of a botnet attack



The BOT problem



Compromised Credentials

LinkedIn – 117 million account (2012)

Yahoo – 3 billion accounts (2013)

eBay – 145 million accounts (2014)

Talk Talk – 157 thousand accounts (2015)

Uber – 57 million accounts (2016)

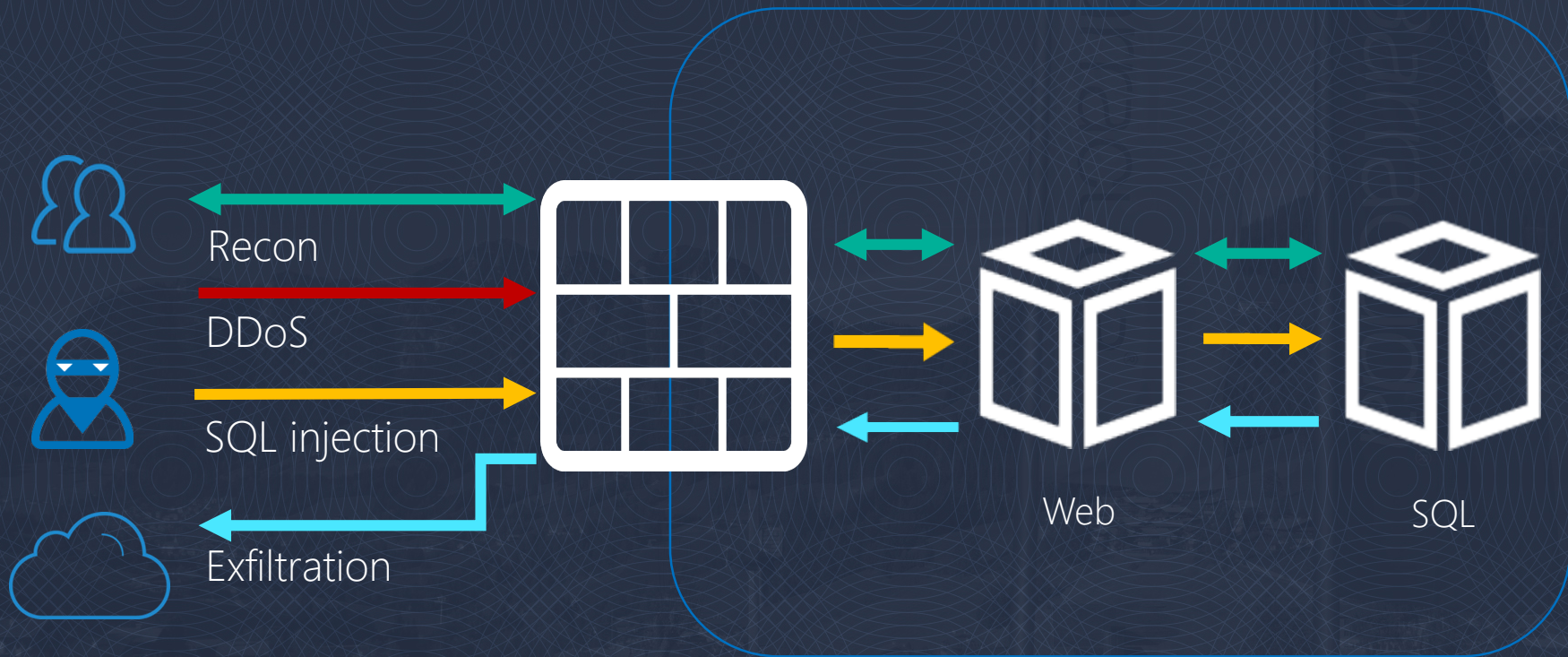
Equifax – 189 million accounts (2017)

Marriott International – 500 million accounts (2018)

<https://haveibeenpwned.com/>



TalkTalk 2015



157,000 user accounts compromised



OWASP Top 21 automated attacks

OAT-001
Carding

OAT-002
Token cracking

OAT-003
Ad fraud

OAT-004
Fingerprinting

OAT-005
Scalping

OAT-006
Expediting

OAT-007
Credential
cracking

OAT-008
Credential
stuffing

OAT-009
CAPTCHA
defeat

OAT-010
Card
cracking

OAT-011
Scraping

OAT-012
Cashing out

OAT-013
Sniping

OAT-014
Vulnerability
scanning

OAT-015
Denial of
service

OAT-016
Skewing

OAT-017
Spamming

OAT-018
Foot printing

OAT-019
Account
creation

OAT-020
Account
aggregation

OAT-021
Denial of
inventory



Industry specific use cases

eCommerce

Media

Travel

Government

Classifieds

Finance

Ad networks

Social networks



eCommerce



Account Takeover

- Hack into accounts using credentials purchased on dark web



Carding

- Hackers testing 1000s of stolen credit cards



Web Scraping

- For content, pricing and inventory information



Scalping

- Automated purchases for black market sales



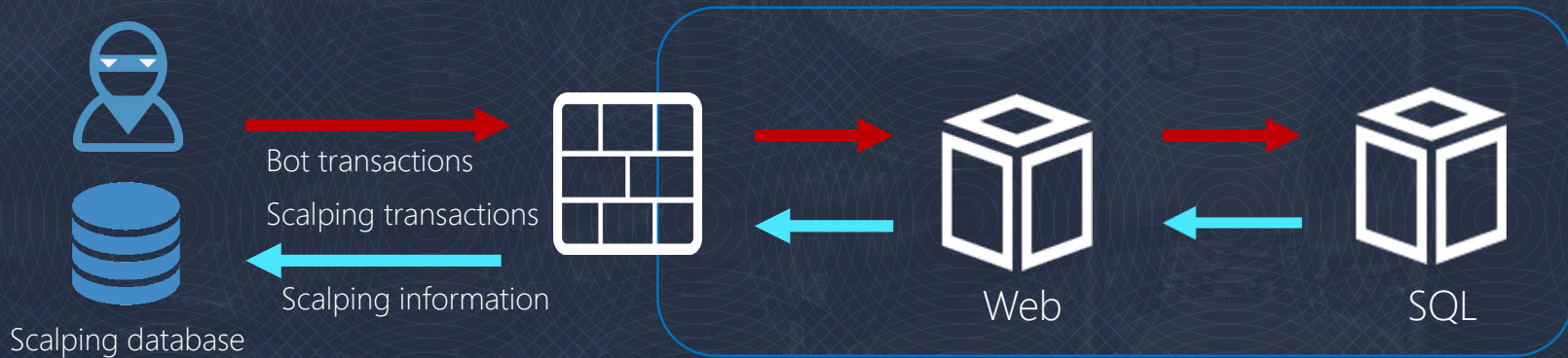
Cart Abandonment

- Add 100s of items to shopping cart and abandon, cause inventory exhaustion



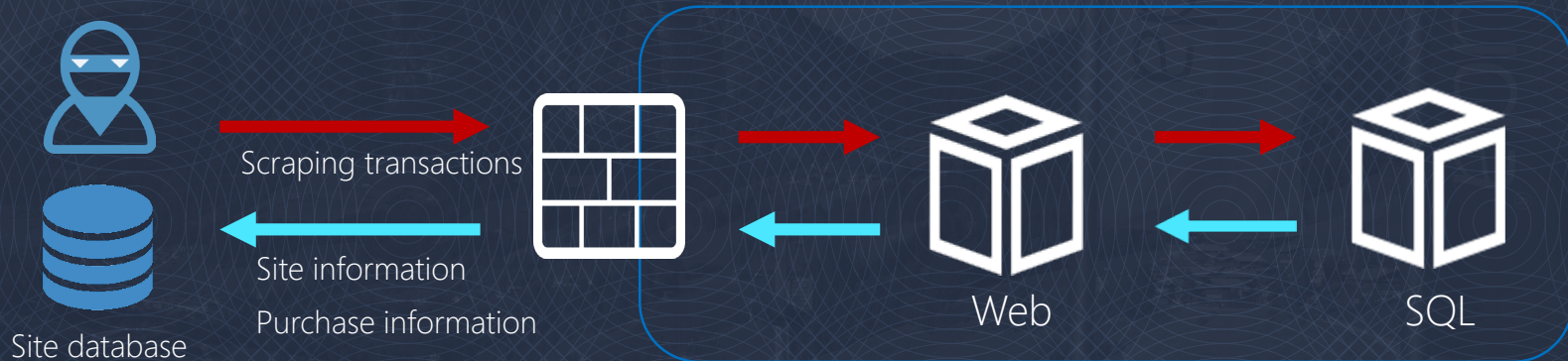
Scalping

Bots take advantage of their speed vs human purchasers to buy a rare resource and then sell at an inflated price



Web scraping

Bots copy data from a website for nefarious purposes such as price fixing, site impersonation, etc.



Finance



Credential stuffing

- Trying 1000s of stolen user credentials



Web scraping

- For content, pricing and inventory information



Application DDoS

- Use layer 7 attacks to DDoS the online service



Account aggregation

- Collect user credentials to access



Government



Comment spamming

- Injecting bad links in comments and review forms



API misuse

- Repeated calling of APIs, loading servers



Application DDoS

- Use layer 7 attacks to DDoS the online service



Account takeover

- Hack into accounts using credentials purchased on dark web



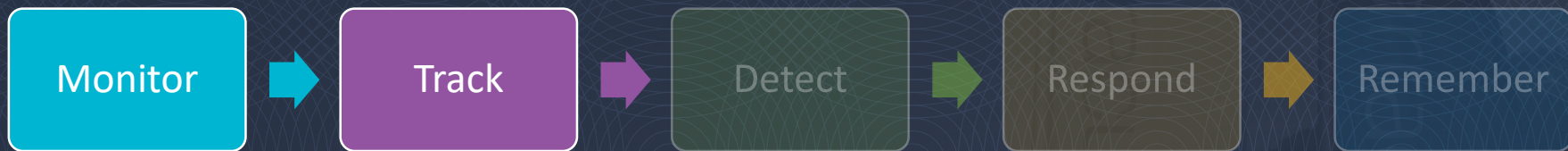
Barracuda Advanced Bot Protection Solution



Solution requirements



Solution requirements : Monitor & track



What WAF had ...

- Web firewall log
- Access logs

Limitations for this task ...

- Number of logs stored
- Limited information about client headers
- Ability to group and correlate logs in sessions

Enhancements ...

- Cloud based storage and analysis engine
- Important information like Header order etc. now captured for analysis



Solution requirements : Detect



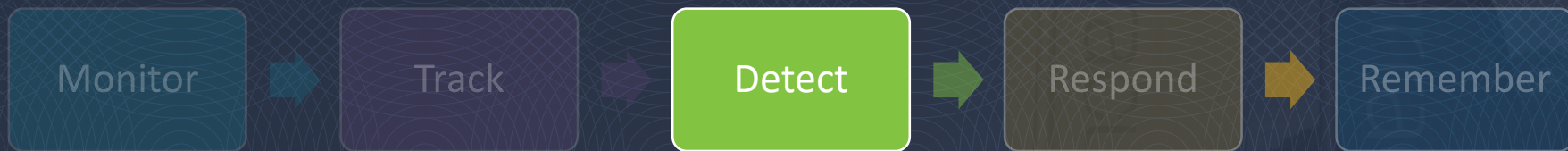
All detections in the WAF were inline

- Features like Brute Force protection requires simple counters

Bot protection requires inline protection & out of band analysis



Solution Requirements : Detect (inline)



What WAF had ...

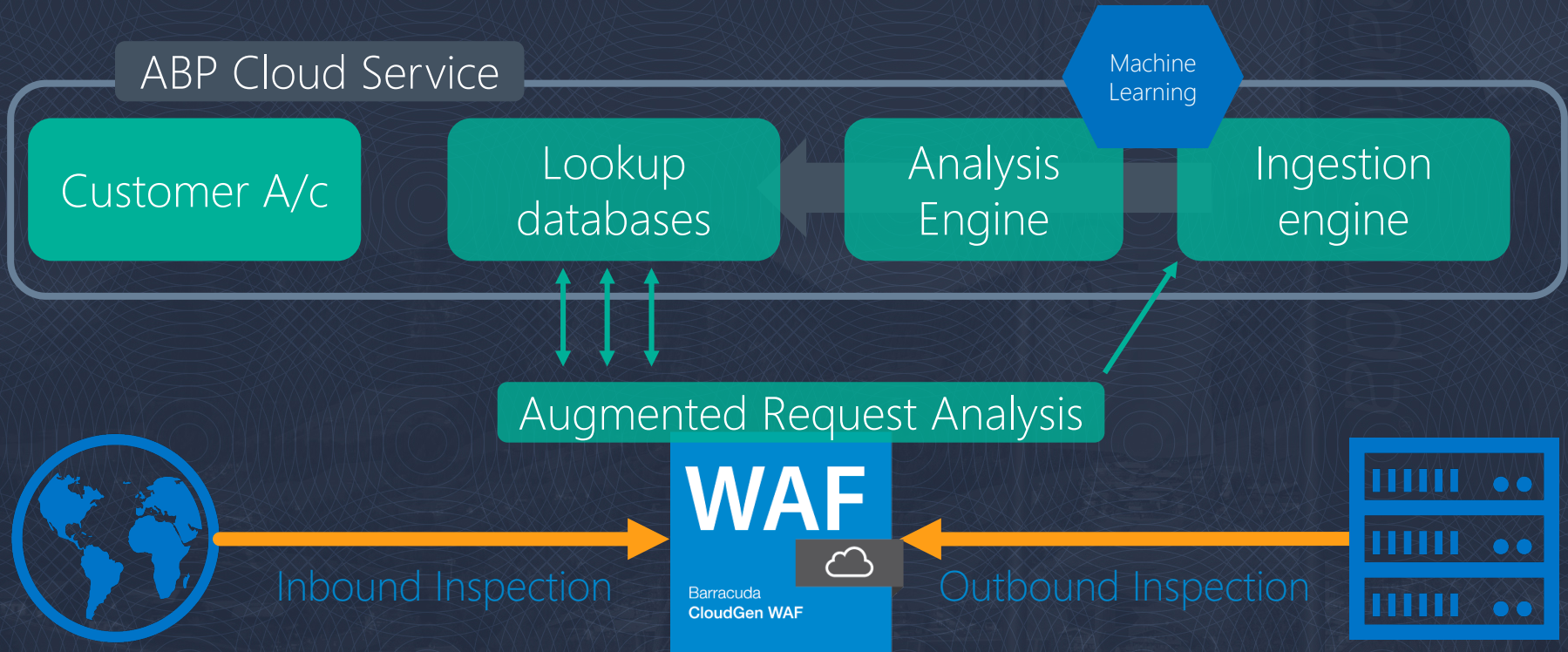
- Brute force prevention
- Web scraping
- Good bot validations
 - rDNS checks
 - IP ranges
- Slow client protection
- Heavy URL protection
- User agent-based tests
- Honey traps using robots.txt

Enhancements ...

- Client Fingerprinting
 - Browser / Headless Browsers / Command-line utilities
 - SSL Fingerprints
- Comment & referrer spam
- Bot signature database



Multi-layer approach for advanced protection



Deployment modes



Barracuda Advanced Bot Detection Cloud

On Premises
(HW / Vx)

IaaS Instances (BYOL)
(Azure / AWS / GCP)

WAF as a
Service

Web Server
module

CDN
plugin

WAF + Bot Protection

Bot Protection Only



Solution Requirements : Detect (out of band)



What WAF had ...

- Nothing

Enhancements ...

- Credential stuffing service
- Data ingestion engine
- Data augmentation
- Analytics for client risk scoring

Road Ahead ...

- Integration with InfiSecure bot engine
- Refining machine learning models for detecting advanced bots



Credential stuffing

Lists of authentication credentials stolen from elsewhere are tested against the application's authentication mechanisms to identify whether users have re-used the same login credentials

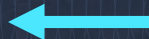
User credential lists



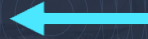
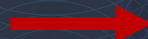
Automated testing

Valid user details

Account takeover



Web



SQL

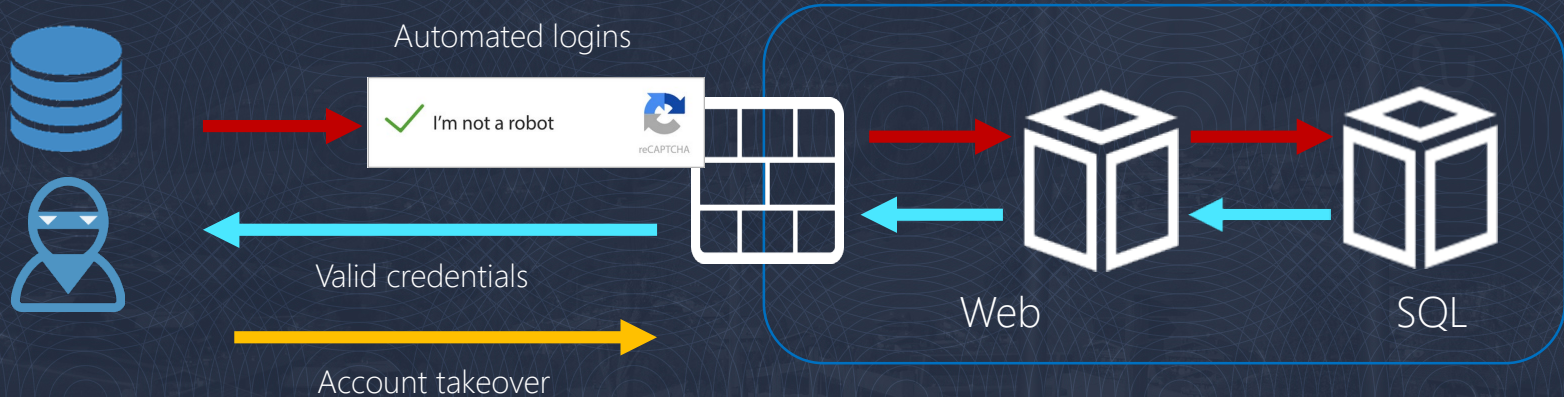


Credential cracking (With CAPTCHA defeat)

Identify valid login credentials by trying different values for usernames and/or passwords.

Additional automation required to defeat CAPTCHA

User account lists



Solution requirements : Respond & remember



What WAF had ...

- Terminate connections
- Block client IP
- CAPTCHA

Limitations ...

- Blocking IP means blocking all NAT'ed clients
- CAPTCHA can be solved using scripts

Enhancements ...

- Blocking devices based on device fingerprints
- Lock out device fingerprints
- Integrate with reCAPTCHA v2
- Maintain client history



Solution requirements



What WAF had ...

- In box security & traffic reports

Enhancements ...

- Built in reports on WAF
- Bot traffic module on the WAF dashboard

Road Ahead ...

- Enhanced cloud bot activity tracking dashboard
- Advanced analytics for application traffic



UI : Bot mitigation tab

BASIC

SECURITY POLICIES

WEBSITES

BOT MITIGATION

ACCESS CONTROL

NETWORKS

ADVANCED

Search help topics

Bot Mitigation

Bot Spam Mitigation

Application DDoS Mitigation

Libraries

Filter default

Bot Mitigation Policy

Preferences

Help

Name	URL Policy	Status	Bot Detection	Account Protection	File Upload Security	Data Theft ...	Options				
default											
test (192.168.0.152:80)							Add				
Host Match: * URL Match: /*	Policy Name: default-uri-... Rate Control Pool: NONE	Statu... Mode...	Web Scra...	Brute Force Preve... Credential Stuffing ...	Anti-virus: On BATP Scan: On	On	Edit	Copy	Rename	Delete	

Web Scraping Policies

Add Policy

Help

Policy Name	Insert Hidden Links	Insert Disallowed URLs	Insert JavaScript	Insert Delay	Delay Time			
test	Yes	Yes	Yes	Yes	10	Edit	Delete	

Session Tracking

Preferences

Help

Name	IP.Port	Session Identifiers	New Session Count	Interval	Status	Options	
default							
test	192.168.0.152:80	PHPSESSID-session		60	On	Edit	



Cloud-based analysis

Summary : Basic Dashboard - Alpha

Access to Dynamic URLs
51,571

Distinct Client IP
217

Unique Devices
304

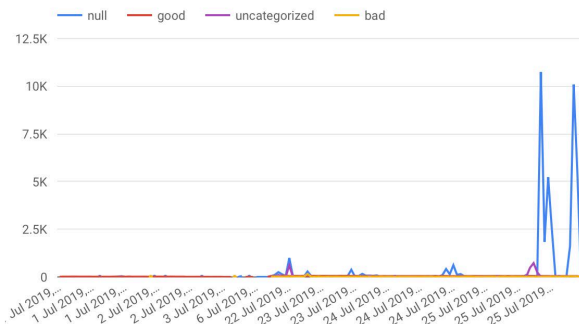
Unique URLs
2,242

User Agents
79

Good Bots
4,731

Bad Bots
1,401

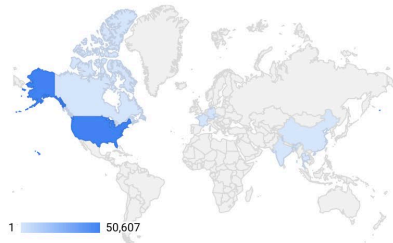
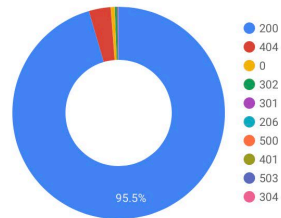
Web Attacks
25,490



Crawler Category	Count
site_monitor	4,615
marketing	1,253
search_engine_bot	168
uncategorised	55
screenshot_creator	1
tool	1
speed_tester	1

1 - 7 / 7 < >

Server Responses



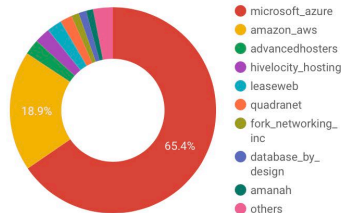
Country	Count
US	50,607
CA	505
DE	271
	135
CZ	32
TH	12
IN	5
CN	3

1 - 9 / 9 < >

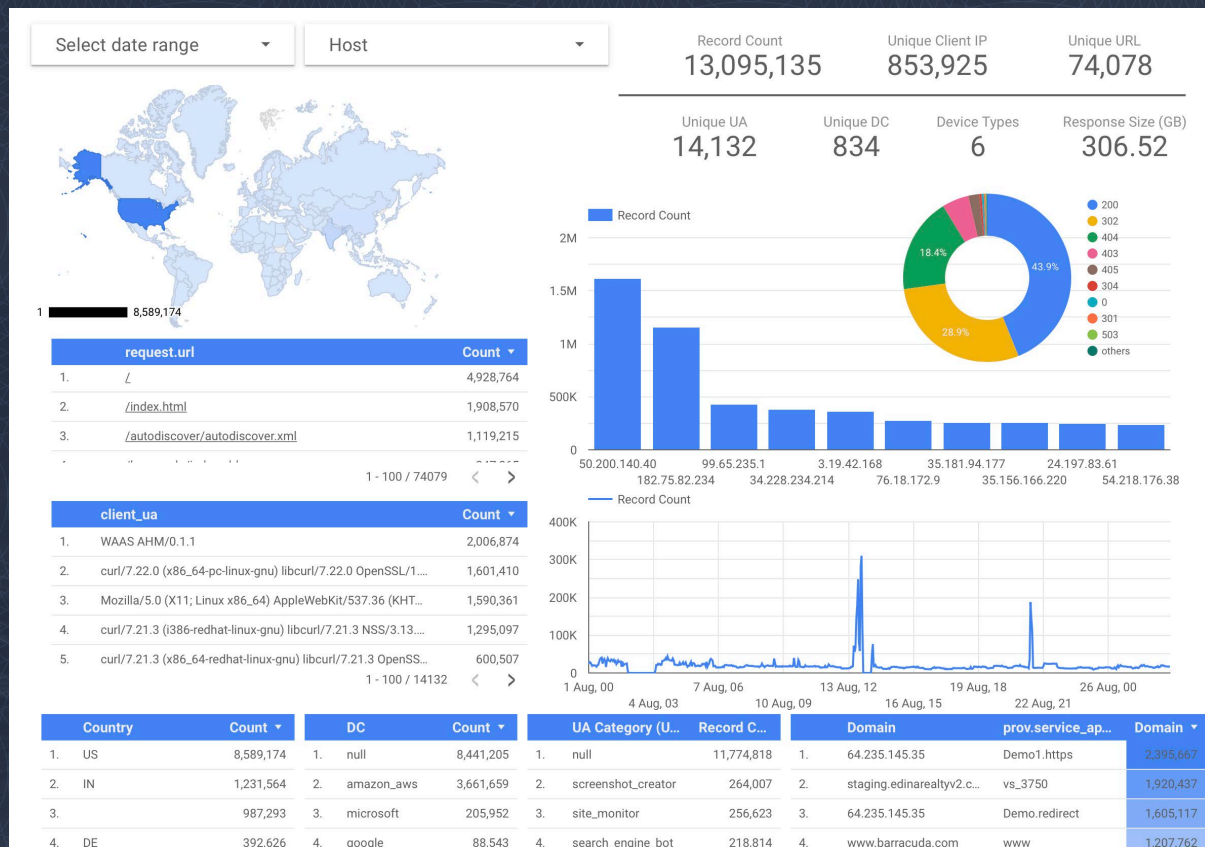
Attack	Count
5	7,506
424	6,497
422	5,312
61	3,193
300	2,370
0	200
145	154
26	143

1 - 16 / 16 < >

Data Centers



Cloud-based analysis



Summary

Bots have direct impact on companies operations, expenses and revenues

Solutions need analyze traffic patterns to effectively block bot protections

Barracuda Advanced Bot Protection

- Can be activated with additional subscription
- Utilizes cloud based engine for advanced analysis
- Provides most effective bot mitigation solution integrated with application security





Thank you

 Barracuda®
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT