black hat®

EUROPE 2017

DECEMBER 4-7, 2017

EXCEL / LONDON, UK

#BHEU / @BLACK HAT EVENTS

Sonia Burney

Solutions Architect
@soniaburney

Brent Maynard

Security Architect
@baammers

Akamai

What is Credential Abuse?

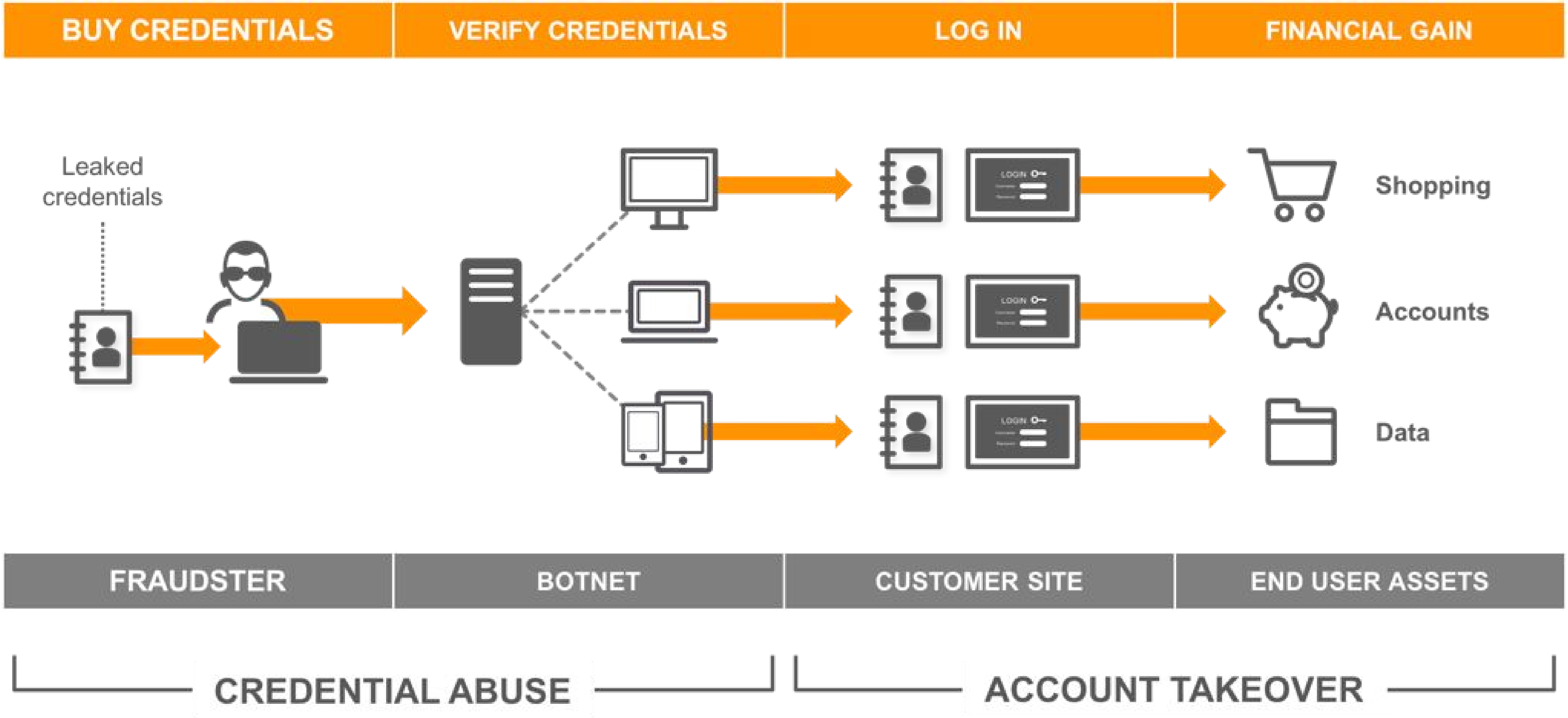
Credential Theft: How do they do it?

Phishing Kits

Keyloggers

Hijack Behavior

Credential Leaks



BUY CREDENTIALS | VERIFY CREDENTIALS | LOG IN | FINANCIAL GAIN

Leaked credentials

Shopping

Accounts

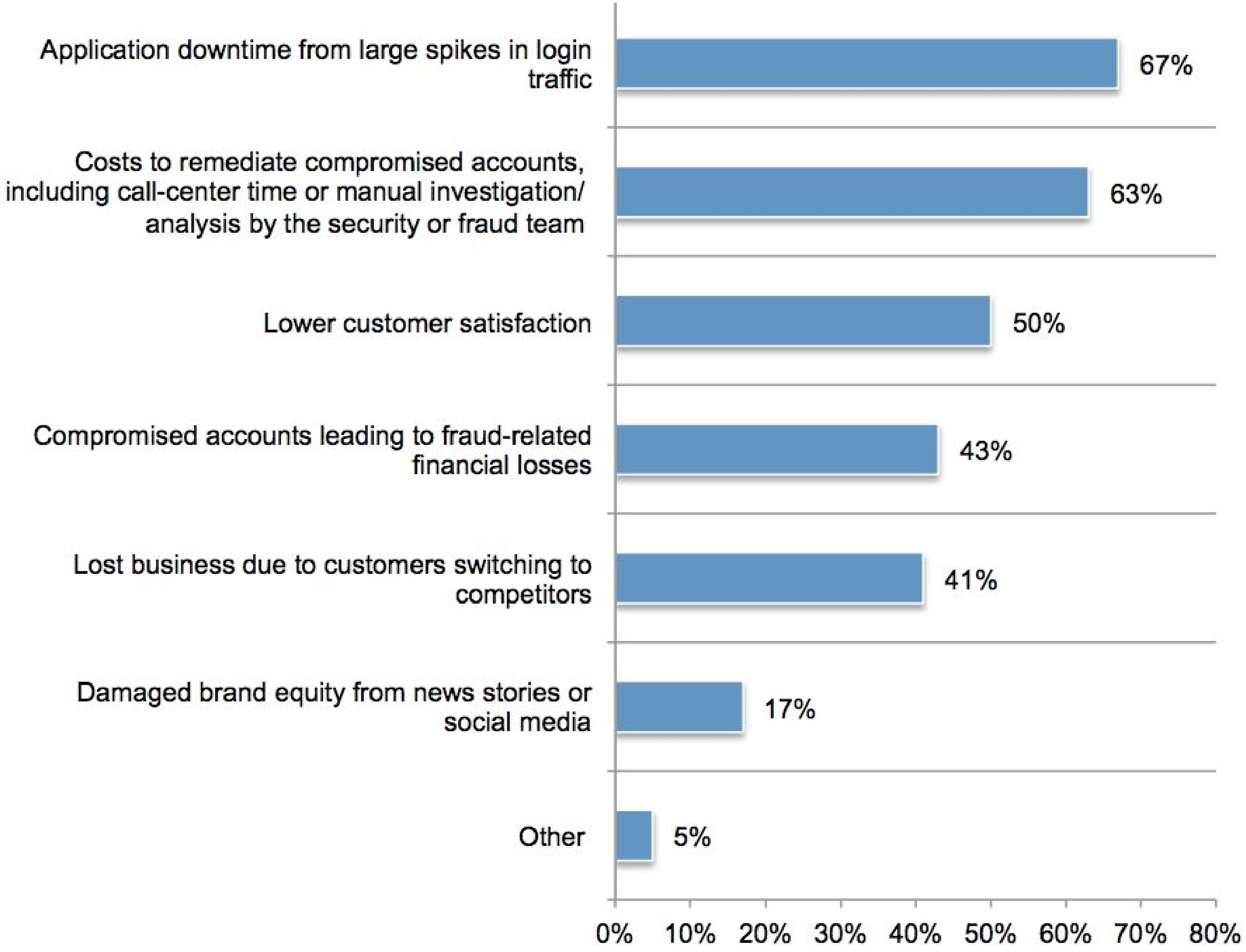
Data

FRAUDSTER | BOTNET | CUSTOMER SITE | END USER ASSETS

CREDENTIAL ABUSE

ACCOUNT TAKEOVER

Negative Consequences Resulting from a Credential Stuffing Attack



Total annualized cost of credential stuffing, excluding fraud, can average more than $6 million

Monetary cost of fraud due to credential stuffing attacks ranges from $546K to $54 million

45 major brand websites

Included retail, banking, travel, media, gaming and other industries

24 hour data collection period during September 2017

420 distinct botnet signatures identified

34,225,052 unique accounts targeted

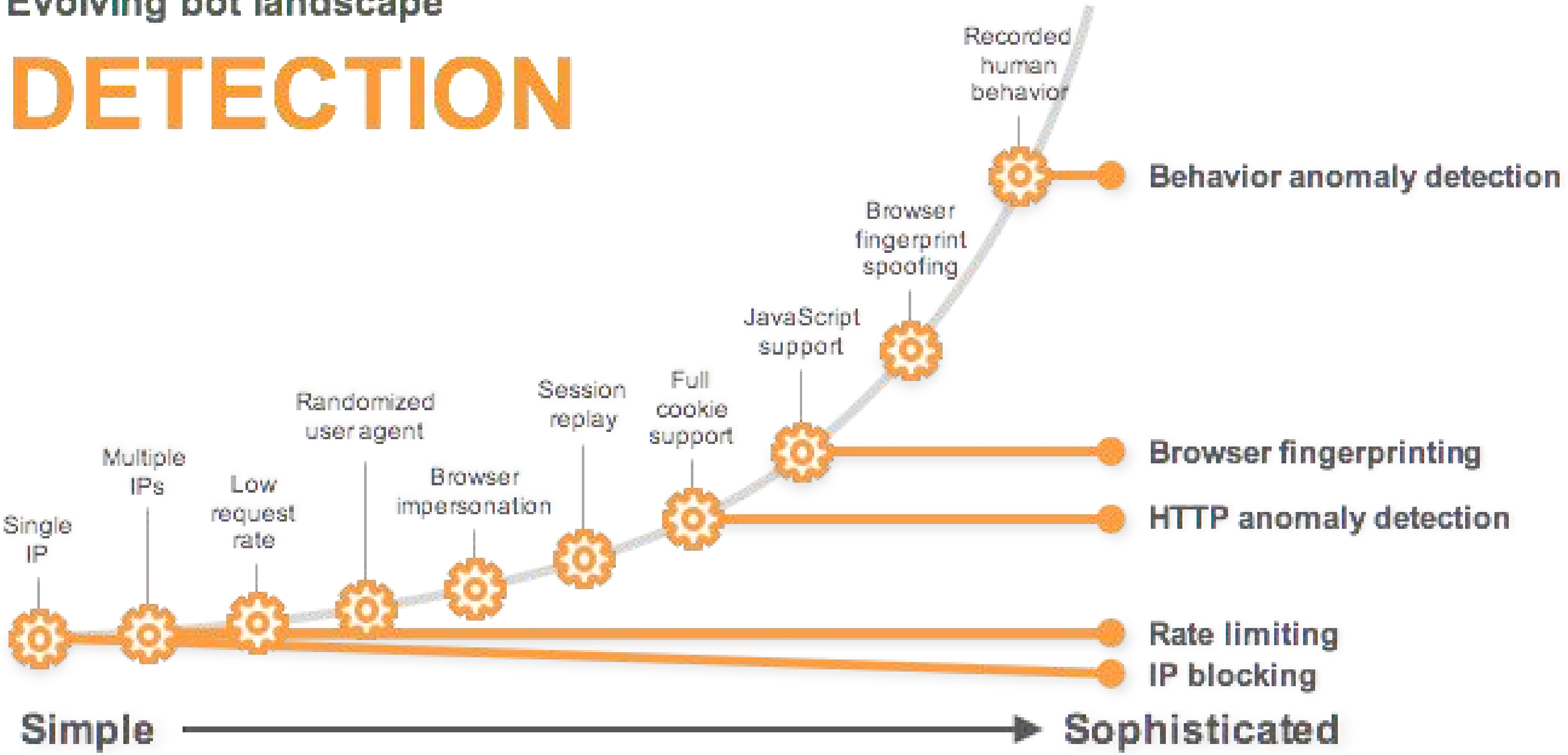
591,774,594 Total logins observed

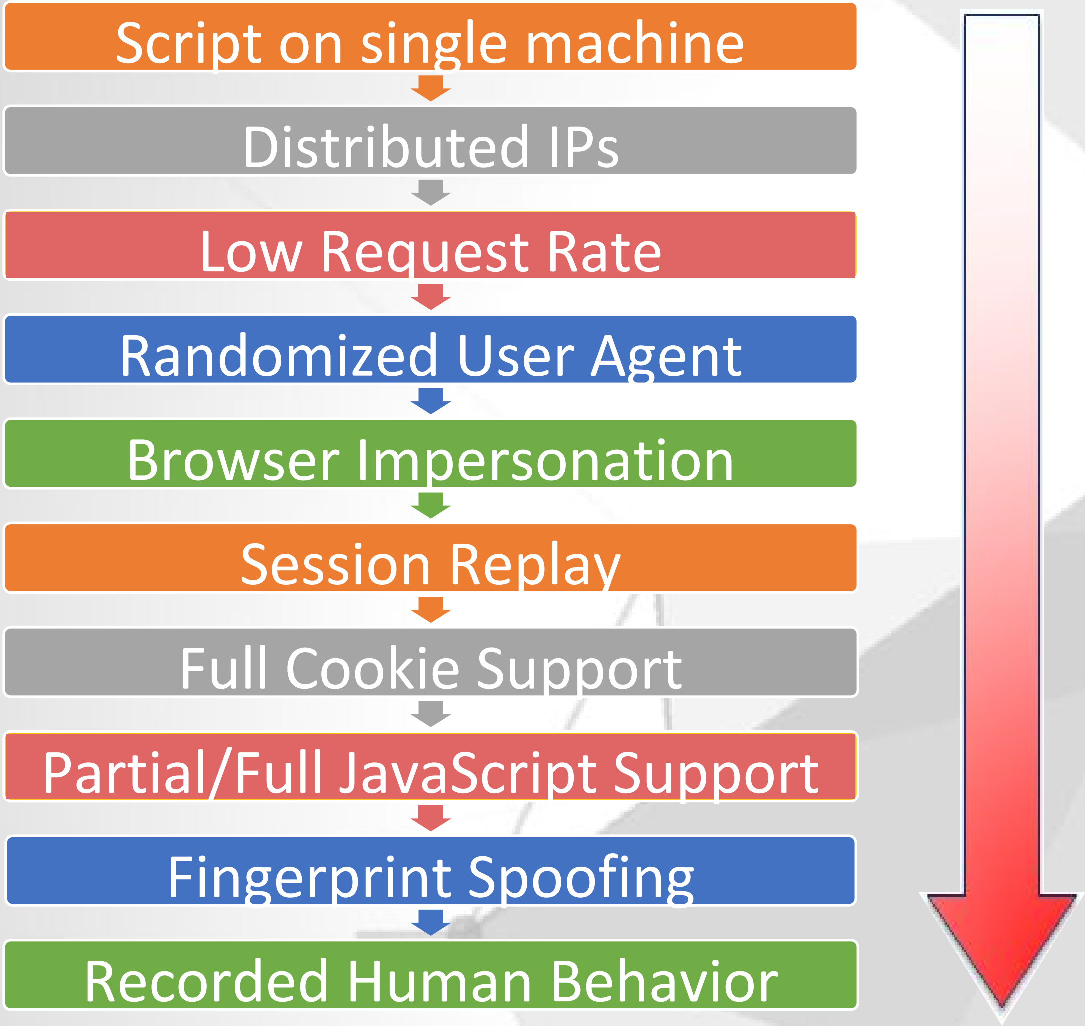
393,924,296 Detected as malicious

66%

Evolving bot landscape

DETECTION





Script on single machine

Distributed IPs

Low Request Rate

Randomized User Agent

Browser Impersonation

Session Replay

Full Cookie Support

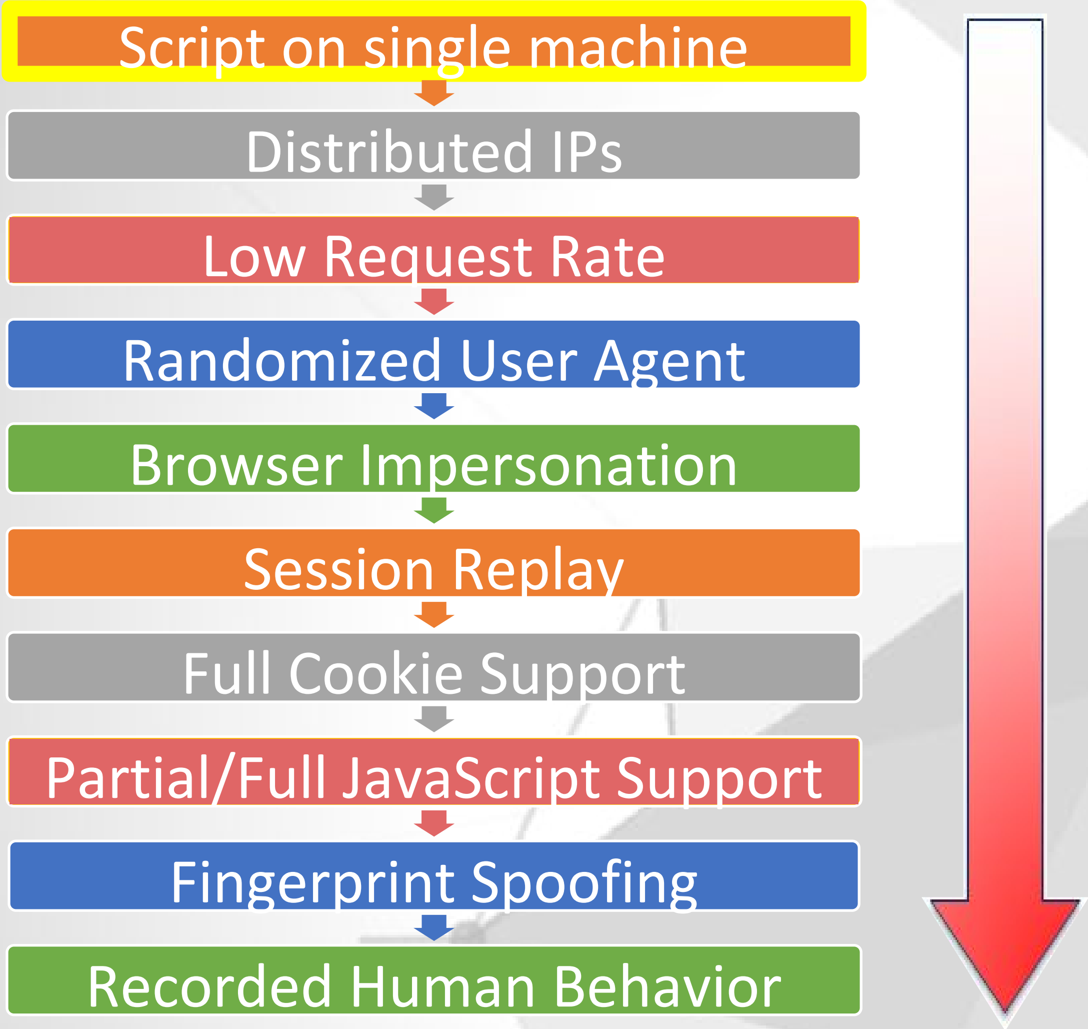
Partial/Full JavaScript Support

Fingerprint Spoofing

Recorded Human Behavior

Simple Bots

Sophisticated Bots

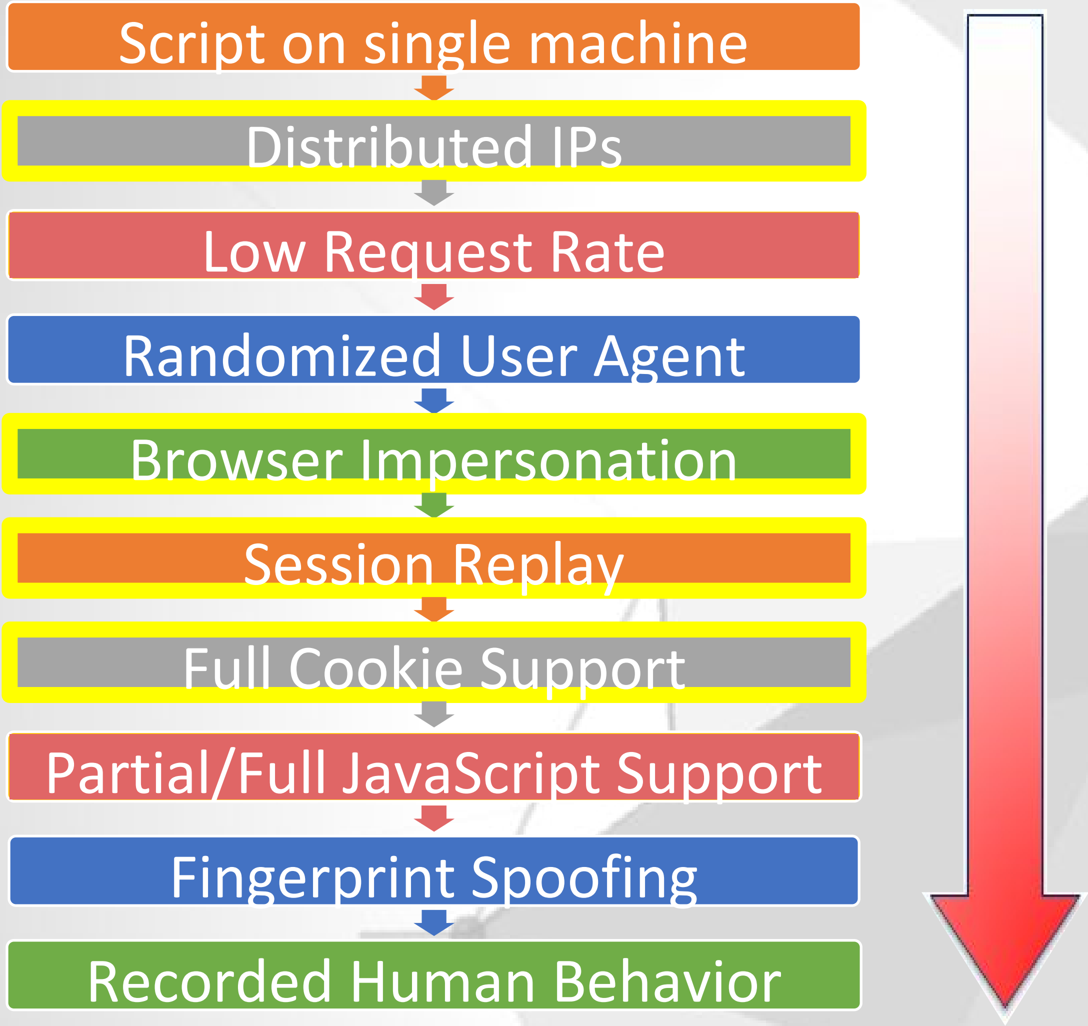


- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

Simple Bots

Rate Detection

Sophisticated Bots



Script on single machine

Distributed IPs

Low Request Rate

Randomized User Agent

Browser Impersonation

Session Replay

Full Cookie Support

Partial/Full JavaScript Support

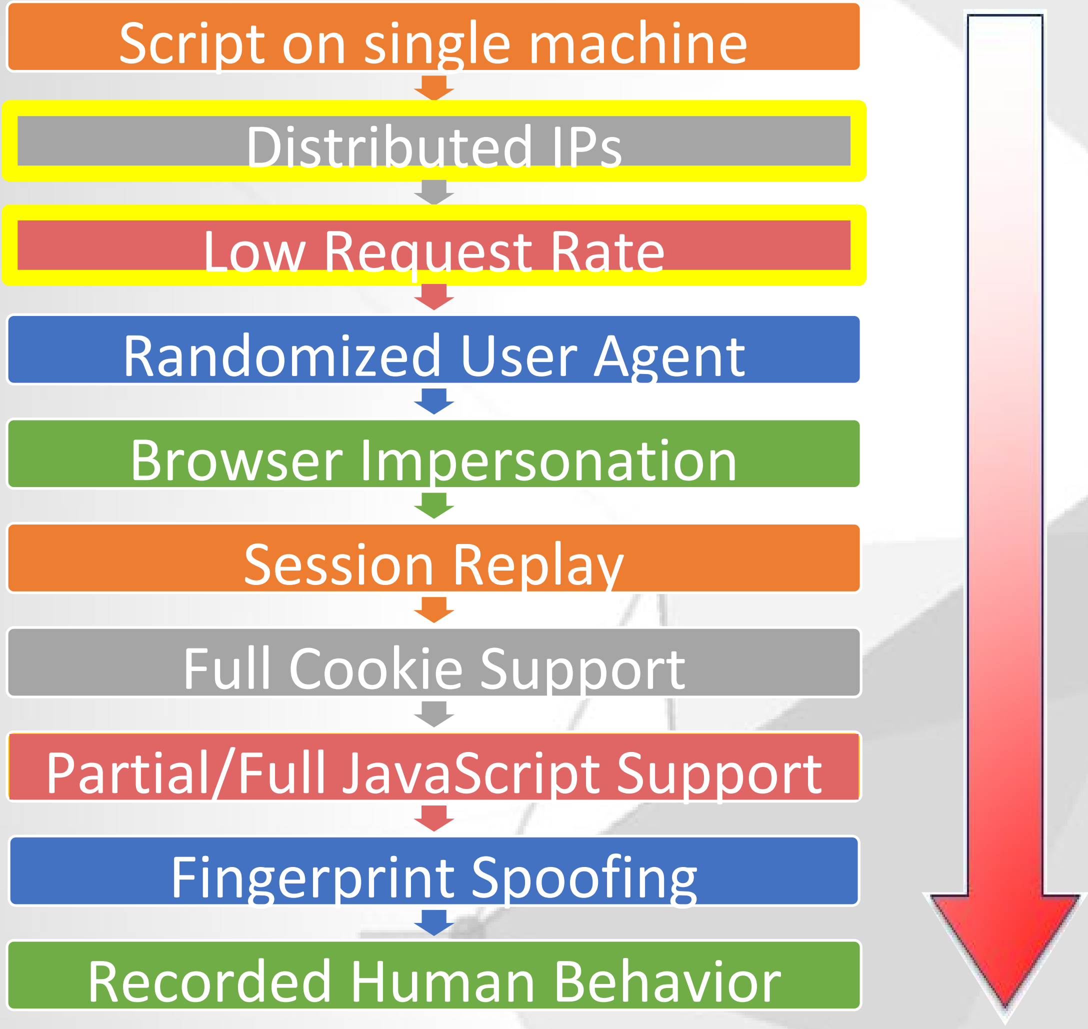
Fingerprint Spoofing

Recorded Human Behavior

Simple Bots

Session Tracking

Sophisticated Bots



Script on single machine

Distributed IPs

Low Request Rate

Randomized User Agent

Browser Impersonation

Session Replay

Full Cookie Support

Partial/Full JavaScript Support

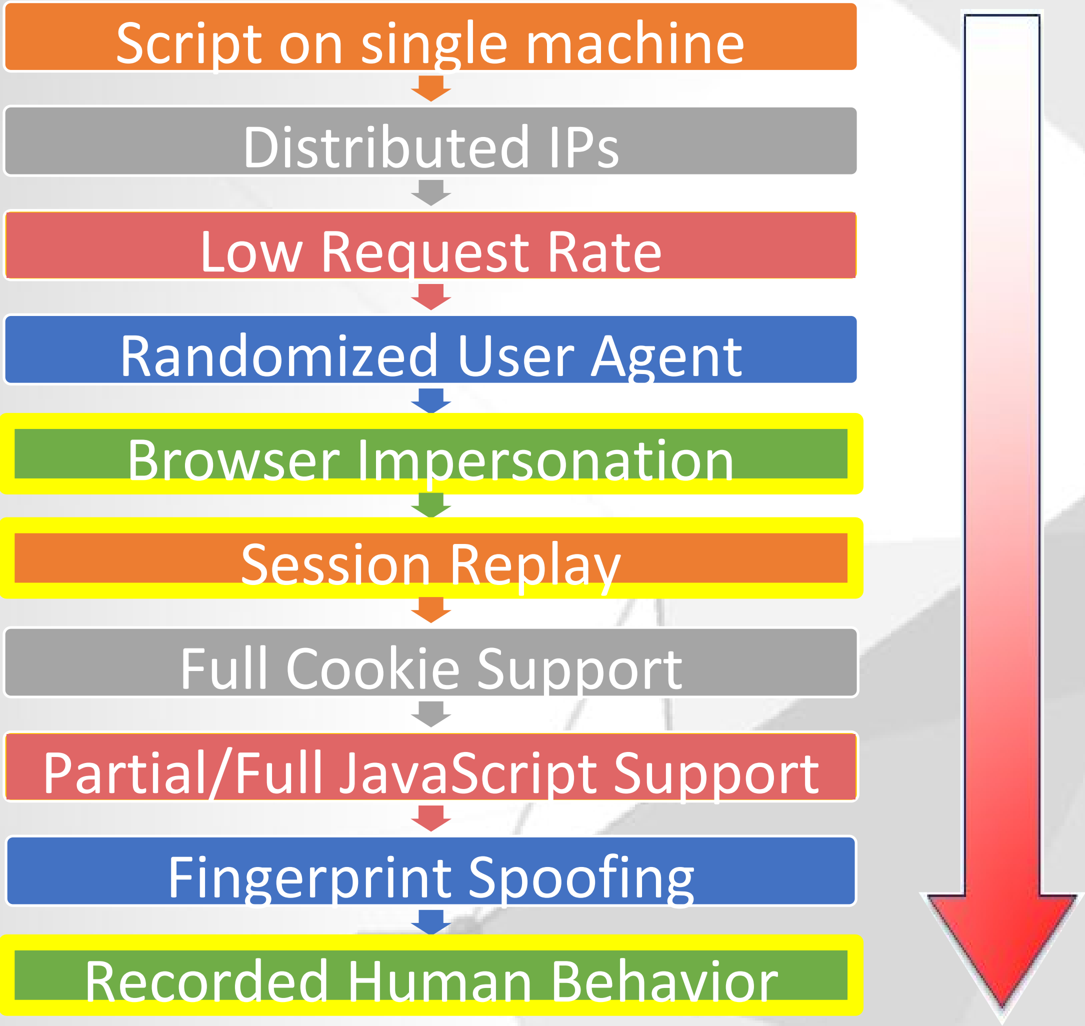
Fingerprint Spoofing

Recorded Human Behavior

Simple Bots

Sliding Window

Sophisticated Bots



Script on single machine

Distributed IPs

Low Request Rate

Randomized User Agent

Browser Impersonation

Session Replay

Full Cookie Support

Partial/Full JavaScript Support

Fingerprint Spoofing

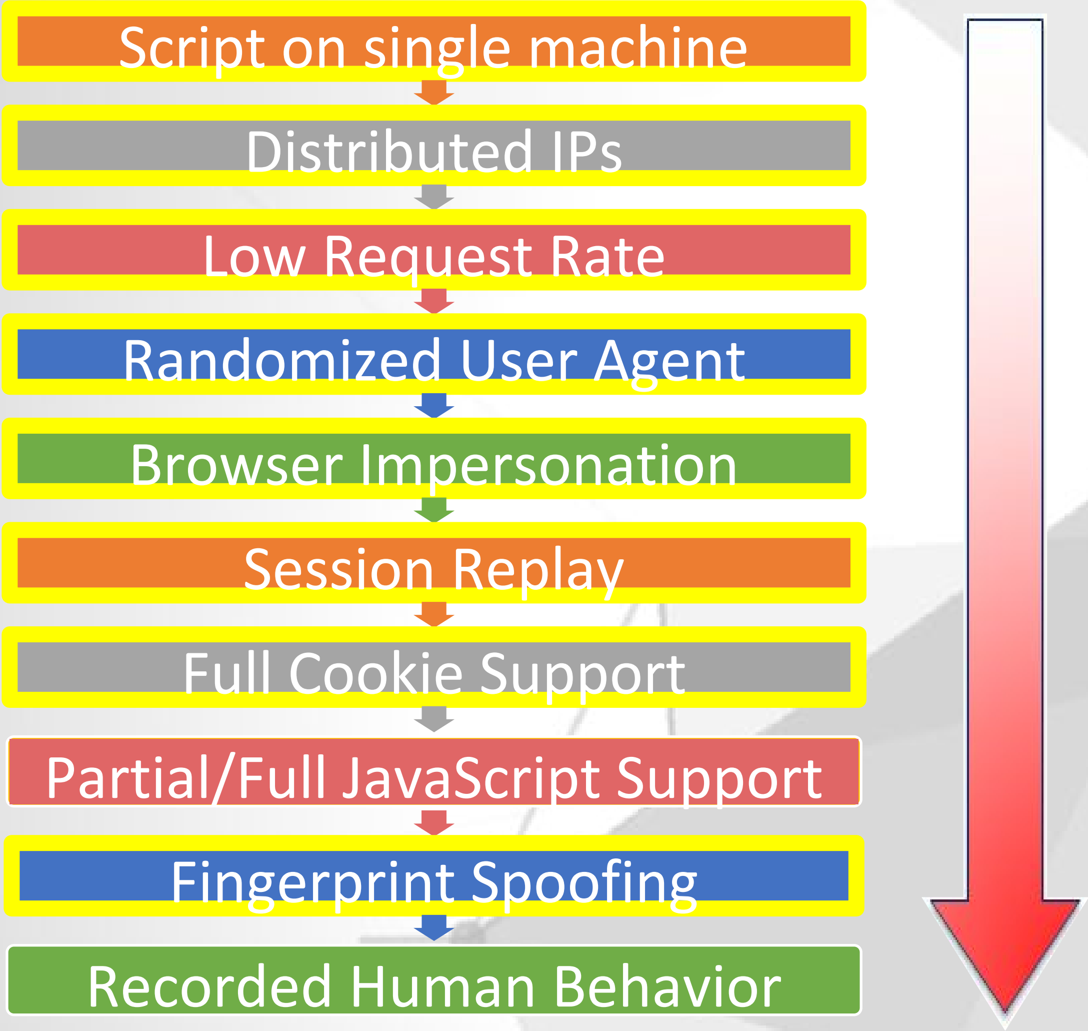
Recorded Human Behavior

Simple Bots

Workflow Validation

Sophisticated Bots

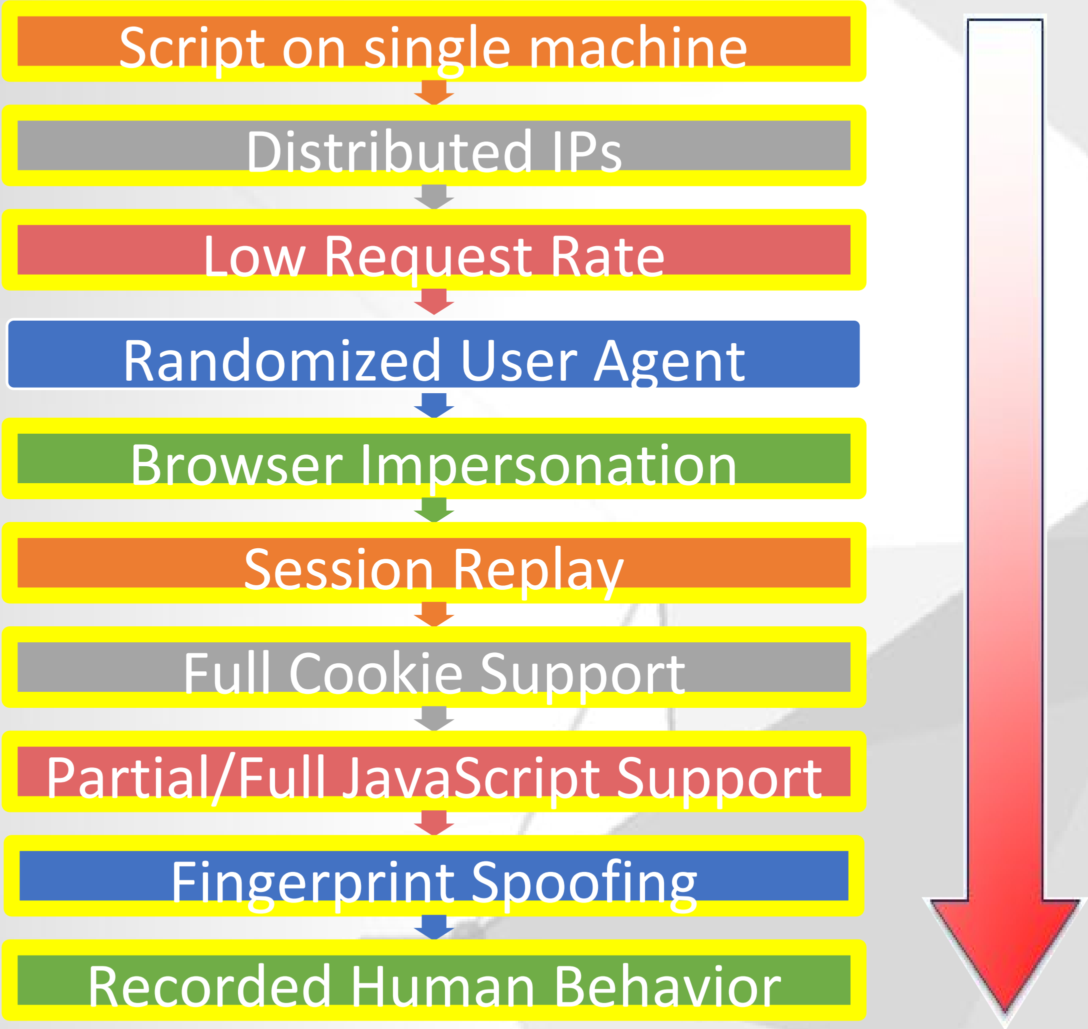
HTTP Anomaly



- Script on single machine
- Distributed IPs
- Low Request Rate
- Randomized User Agent
- Browser Impersonation
- Session Replay
- Full Cookie Support
- Partial/Full JavaScript Support
- Fingerprint Spoofing
- Recorded Human Behavior

Simple Bots

Sophisticated Bots



Script on single machine

Distributed IPs

Low Request Rate

Randomized User Agent

Browser Impersonation

Session Replay

Full Cookie Support

Partial/Full JavaScript Support

Fingerprint Spoofing

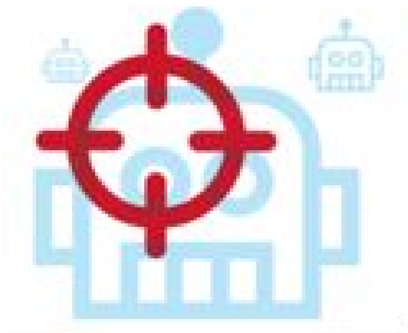
Recorded Human Behavior

Simple Bots

Behavioral Detection

Sophisticated Bots

Evolution of Bot Detection and Mitigation Approach



Identify

Delay: 1-3s

Slow: 8-10s

Customized Content

Block

Takeways...

- One password to rule them all?
  - Understand ***<u>ALL</u>*** login processes and policies
- Understand what real users and bad actors look like
- Identify multiple detection and mitigation strategies
- Foreshadowing the credential abuse landscape

Next Steps...

- Pivot in focus of threat surface
- Growth of API/IoT traffic
- Expansion of Native Application Endpoints
- AI and Machine Learning