

# BOTS DOWN UNDER

[ AN AUSTRALIAN MARKET THREAT REPORT ]

April 2019

kasada

Copyright © Kasada Pty Limited 2019

<b>INTRODUCTION</b>	04
<b>EXECUTIVE SUMMARY</b>	06
<b>METHODOLOGY</b>	10
<b>FINDINGS</b>	12
<b>ACTION PLAN</b>	16
<b>ABOUT KASADA</b>	18
<b>APPENDICES</b>	20
How attacks happen	20
How attackers work	22

# INTRODUCTION.

Many aspects of our lives are global – especially security.

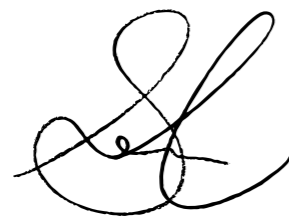
But the world is not homogeneous.

Local still matters.

This report reveals aspects of the threat landscape, distinct to Australia, that local businesses need to know. They are either overlooked or misunderstood in global reports published by overseas vendors.

Kasada kicked off in Australia and we're uniquely placed to see and comment on the threat of malicious automation.

We take our role in the Australian security community seriously. And we hope this report contributes to a safer, more secure environment for all.



- Sam Crowther - CEO, Kasada



# EXECUTIVE SUMMARY.

Last year was a big year for bots in Australia.

In 2018, Kasada stopped a wide variety of attacks. The most prevalent and damaging were those that exploited stolen user credentials to access accounts.

The business cost of these attacks is becoming well documented and includes:

- Economic – an estimated average of \$2m per breach<sup>1</sup> of time, compensation and customer churn.
- Reputational – reporting of data breaches often results in damaging publicity. There were 749 reported in 2018, with credential abuse the third largest reason<sup>2</sup>.

Two factors drive the popularity with criminal gangs of this attack type:

- An estimated 6.7 billion stolen credentials available online to exploit<sup>3</sup>.
- A low barrier to exploitation. Attacks are automated using bots and once initiated they happen at scale, persistently and without human involvement.

*Bots Down Under* reveals two specific, actionable issues that Australian businesses need to address:

1. **BOT VISIBILITY**

- **90% of the country’s leading 250 websites do not see the difference between bots and customers.**
- This leaves bots free to persist, unassailed, eating up bandwidth, spiking server costs and slowing down sites.

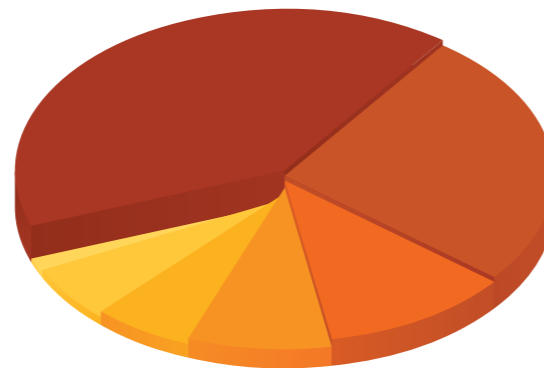
2. **BOT GEOGRAPHY**

- **90% of credential abuse attacks come from Australian networks**
- This debunks the theory of “Island Australia”. It is no longer sound strategy to geo-block overseas traffic and assume local traffic is legitimate.

Kasada’s conclusion – urgent action is needed to keep Australian businesses up to pace with the threats bots pose.

## OFFICE OF AUSTRALIAN INFORMATION COMMISSIONER SOURCES OF THREATS 2018

<b>Phishing</b>	<b>122</b>	(41%)
<b>Compromised Creds</b>	<b>77</b>	(26%)
<b>Bruteforce</b>	<b>34</b>	(11%)
<i>(Credential Abuse)</i>		
<b>Hacking</b>	<b>26</b>	(9%)
<b>Malware</b>	<b>19</b>	(6%)
<b>Ransomware</b>	<b>17</b>	(5%)
<b>Other</b>	<b>5</b>	(2%)



<sup>1</sup> [Cost of a Data Breach Study](#), Ponemon, 2018 | <sup>2</sup> [OAIC](#), Dec 2018 | <sup>3</sup> [Have I been pwned?](#)

## FIGURES SHOW AUSTRALIAN DATA BREACHES ON THE RISE

- [Australian Financial Review](#) Feb, 2019

FINANCIAL REVIEW

## MARRIOTT'S STARWOOD HACK HITS UP TO 500 MILLION CUSTOMERS

- [Australian Financial Review](#) Dec, 2018

FINANCIAL REVIEW

## CATHAY PACIFIC STOCKS PLUNGE AFTER AIRLINE REVEALS MASS DATA BREACH BY HACKER

- [ABC](#) Oct, 2018

ABC NEWS

## AUSTRALIAN BANK CUSTOMERS CAUGHT IN VALUATION FIRM DATA BREACH

- [IT News Australia](#) Feb, 2019

itnews

# METHODOLOGY.

## BOT VISIBILITY

### QUESTION

What percentage of Australia's leading websites can differentiate between browsers (people) and scripts or automation tools (bots)?

### SAMPLE

We assessed the top 250 Australian websites, based on Alexa ranking.

We focused our research on the industries most often targeted by bot attacks: retail, property, wagering, finance, airlines, utilities and health insurance.

### APPROACH

We used three different tools to load a login page and submit test credentials:

1. A browser.
2. A script – curl or Node.js.
3. An automation tool – Selenium or headless browser.

These three tests use common, benign tools to simulate the capability of the common credential abuse tools. This allowed us to assess whether a website could prevent a credential abuse tool from submitting requests. At no stage did we use a malicious tool or send any malicious requests.

## BOT GEOGRAPHY

### QUESTION

How are credential abuse attacks delivered to Australian companies?

### SAMPLE

We thoroughly analysed every credential abuse attack targeting Kasada customers last year.

In total we captured data of more than 100 attacks. Credential abuse attacks are an emerging attack type. The 2018 OAIC statistics included 34 incidences; so this sample represents a significant insight into a growing problem.

### APPROACH

We evaluated key characteristics including: attack tool identification, proxy network analysis, attack thresholds, http header analysis and advanced telemetry analysis.

We mapped the geography, network owner and connectivity profile of the proxy ip addresses.

# FINDINGS.

## BOT VISIBILITY

**86%** OF THE TOP 250 WEBSITES FAILED TO DETECT A SCRIPT LOADING THE LOGIN PAGE

- This showed there was no security control in place to differentiate between browsers and scripts.
- If we could load a page with a curl request, an attacker could also load the page with a credential abuse tool.

**90%** FAILED TO PREVENT AN AUTOMATION TOOL FROM SUBMITTING CREDENTIALS

- This showed there was no security control in place on the backend system.
- Tools such as Selenium provide significant automation power that is used for both good and bad.

### ANALYSIS

A website that fails to detect a curl request will equally be unable to differentiate between SentryMBA, SNIPR and a regular browser.

86% of the websites we tested failed to make this differentiation. There are a number of possible reasons why the results are so high.

1. Credential abuse attacks are relatively new and businesses have not properly assessed their risk exposure.
2. Businesses mistakenly believe their web application firewall will prevent these attacks.
3. Companies are relying on reactive controls, including password locks, or fraud systems.

Connecting the dots between stolen credentials, inability to mitigate bot attacks, and the Office of Australian Information Commissioner (OAIC) data breach notification statistics is a key outcome of this research. A staggering 86% of Australian websites lack a proactive control to the third most common reason why data breach attacks occur.

For executives keen to avoid contributing to next quarter's OAIC statistics, we definitely advise you understand your risk exposure to these attacks.

We are deliberately not disclosing any results specific to customers or even industry verticals. This is not an exercise in publicly outing individual businesses. We are simply highlighting a risk that has elevated significantly in the past year.

# FINDINGS.

## BOT GEOGRAPHY

**90%** OF CREDENTIAL ABUSE ATTACKS ARE SENT VIA AUSTRALIAN ISP NETWORKS

The remaining 10% used international networks of infected machines.

### ANALYSIS

Attacks are being delivered from within Australia's own backyard. This flies in the face of the threat intelligence provided by international vendors. It also makes the task of detecting these attacks significantly harder.

The modus operandi of most adversaries is to avoid detection for as long as possible by mimicking users.

Their techniques include:

- Creating login requests identical to users.
- Sending their requests from the same ISP networks.
- Knowing that each IP address only submits a small number of requests.
- Rotating http headers or pretending to be common browsers.
- Following Australian daylight hours.

These tactics often result in the attacks lasting days or weeks before being detected. Many organisations will need to rethink their approach to attack visibility, in order to effectively address this threat.



# ACTION PLAN.

Defeating the credential challenge requires a multi-pronged approach.

- Individuals need to stop reusing passwords.
- Security versus user experience impact of multi-factor solutions needs to be assessed.
- Web security industry needs to evolve, with the help of innovative startups, to defeat fraudulent bot attacks.
- Businesses need to address the risks associated with bot attacks.
- Security teams need to add a dimension to their attack visibility.

## FOR INFOSEC:

### ASK THESE HARD QUESTIONS:

- Do we actively monitor failed login requests?
- Do we actively monitor account locks and password resets?
- Is there a feedback loop between infosec and the call centre to report on account locks?
- Do we actively monitor how often an account is logged into?
- Do we actively monitor how often an IP address submits a login request?
- Do we understand the expected request flow pattern of the login process?
- Are we monitoring for deviations from this pattern?

### TAKE THESE PRECAUTIONS:

- Only allow browsers to access your web login page.
- Enforce adherence to request flow patterns.
- Take actions to alter the economics of attacking your site.
- Visualise the human versus bot activity against your login paths.

## FOR THE BUSINESS:

### ASK THESE HARD QUESTIONS:

- Do we understand the potential impact of an attack against a customer portal?
- What personal user data (PII) is available in a customer portal?
- Does the portal allow for the extraction of funds or anything of value?
- Have we calculated the hard and soft costs of responding to a breach?
- Do we have visibility of the health of our portal accounts?
- Can our infosec team report on login activity?

### TAKE THESE PRECAUTIONS:

- Establish a regular cadence of reporting on these issues.
- Ensure the necessary security controls are in place.
- Have a data breach response plan established and tested.

# ABOUT KASADA.

Leading Australian organisations – including ASX100 companies – trust Kasada to protect them.

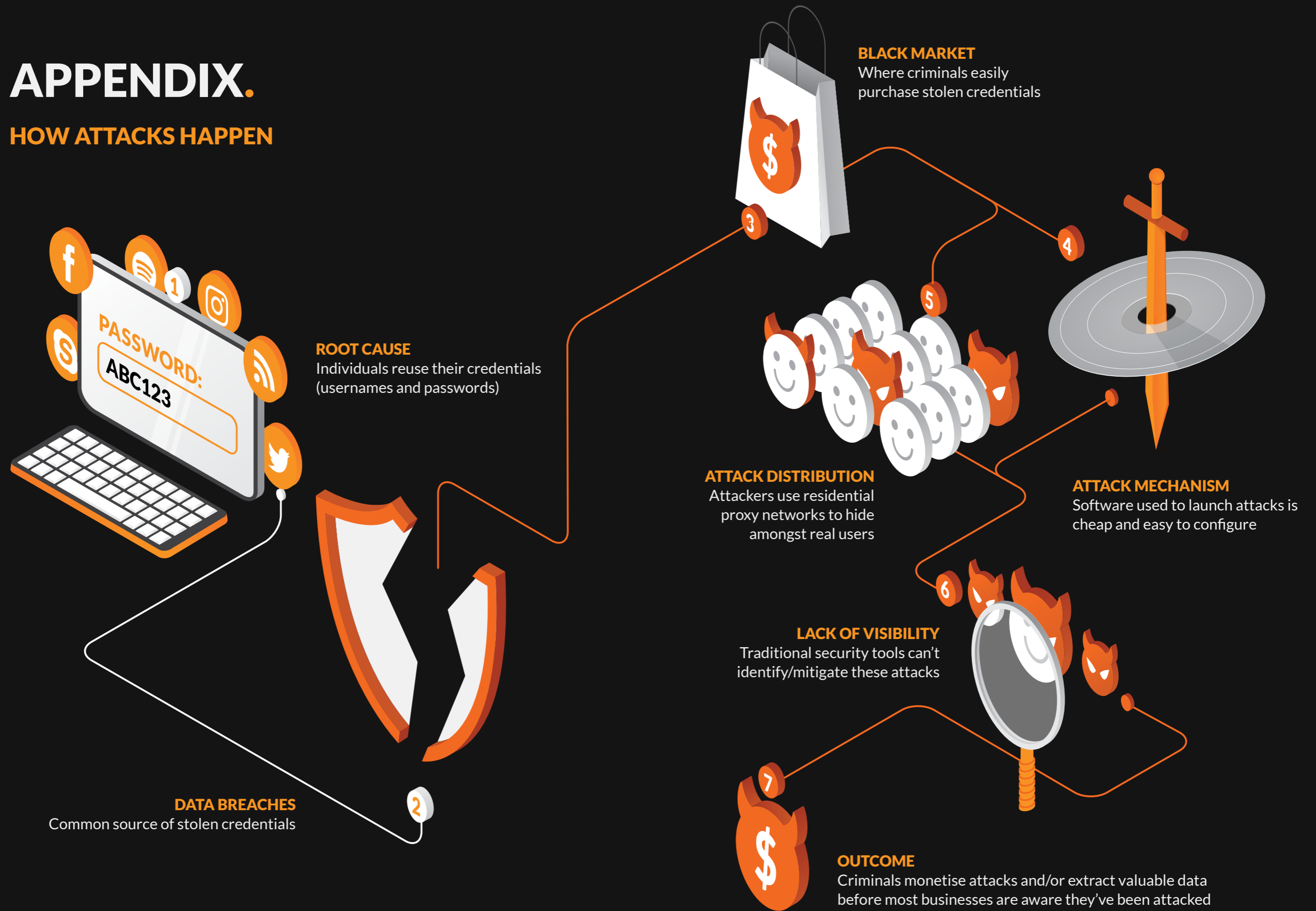
Kasada is backed by leading Australian venture capital firms, and the Federal Government's [Accelerating Commercialisation Program](#).

Kasada understands the security landscape of Australia like few others and deploys to businesses under attack within hours.

For more information visit [www.kasada.io](http://www.kasada.io), to request a demo [www.kasada.io/demo/](http://www.kasada.io/demo/)

# APPENDIX.

## HOW ATTACKS HAPPEN



# APPENDIX.

## HOW ATTACKERS WORK

Attackers typically follow these six steps:

### 1 OBTAIN THE DATA SET

These are usernames/passwords easily sourced from data breaches.

### 2 ASSESS THE ENVIRONMENT

Most primary websites are targeted in 95%+ of attacks. Why? They're easiest to find and it's simple to extract the request data from a browser. Attackers will only look for another way in if they fail at the primary site.

### 3 SELECT YOUR ATTACK TOOL

Tools such as SentryMBA, SNIPR or Cr3d0c3r make attacks simple and cheap to launch. They typically come with existing configurations, Youtube tutorials and online user forums. They also have deceptive features, such as http header rotation, proxy rotation, and captcha evasion.

### 4 LAUNCH SIMULTANEOUS ATTACKS

Most attack patterns point to campaign-based activity. And they're typically organised by industry or sector. This increases attackers' efficiency and effectiveness.



### 5 LEVERAGE RESIDENTIAL PROXY NETWORKS

Attackers use proxy networks to distribute attack load and mask their true location. Most modern proxy networks will allow you to specify the country and the class of IP – data centre, domestic ISP or mobile carrier IP. This allows attacks to hide within the same ISPs as the target's customers.

### 6 EXTRACT DATA AND MONETISE

In many cases, data extraction occurs without any resistance from the target as they are unaware of the nefarious activity. Where monetisation is possible, this can occur within 60 minutes.

EMAIL

info@kasada.io

WEB

1300 76 86 01

AUS PHONE

kasada

Copyright © Kasada Pty Limited 2019