REPORT

Understanding Credential Stuffing Attacks:

A REAL-WORLD EXAMPLE

Introduction

As the world continues to see an incredible spike in legitimate, digital consumer activity, it's accompanied by a similar spike in fraudulent activity. The surge in online traffic makes it more difficult to identify malicious behavior, which becomes a needle in the proverbial haystack of web traffic.

One of those malicious behaviors is credential stuffing, an increasingly popular automated threat. Understanding how these types of cyber threats evolve over time, as bad actors hone their weapons to successfully break through a company's defenses, is essential to protecting your most fundamental assets: your brand reputation, customer loyalty, and ultimately revenue. Here we present our analysis of a real-world attack that we monitored for one of our retail customers using Kasada.

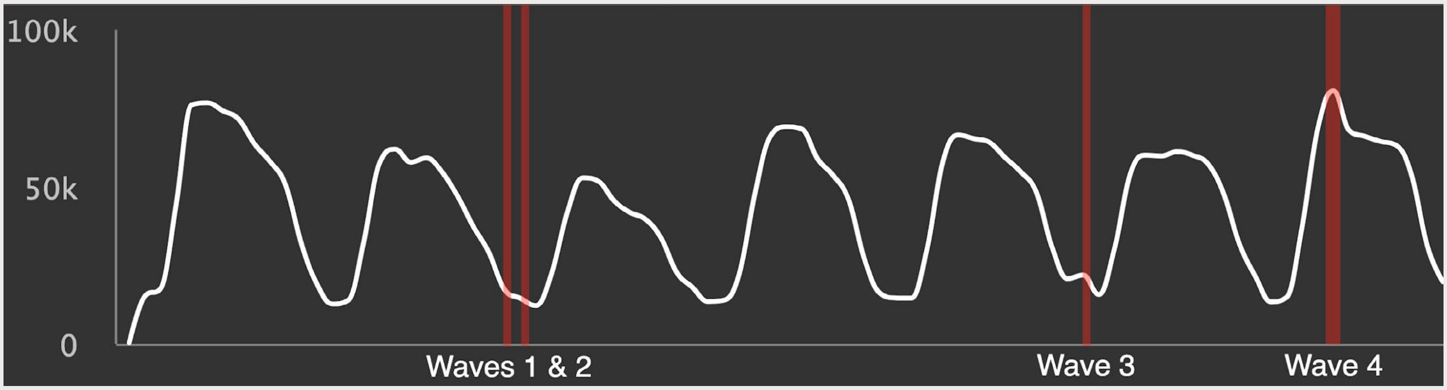
Three Waves of Attack

Recently, we came across a sophisticated threat actor targeting a retail organization's eCommerce applications. This particular actor was attempting to use stolen credentials to gain unauthorized access to customer accounts. During the period of time we observed this attack, we identified three distinct waves:

First wave: Standard adversarial tooling

Second wave: Retooling attempt #1

Third wave: Retooling attempt #2



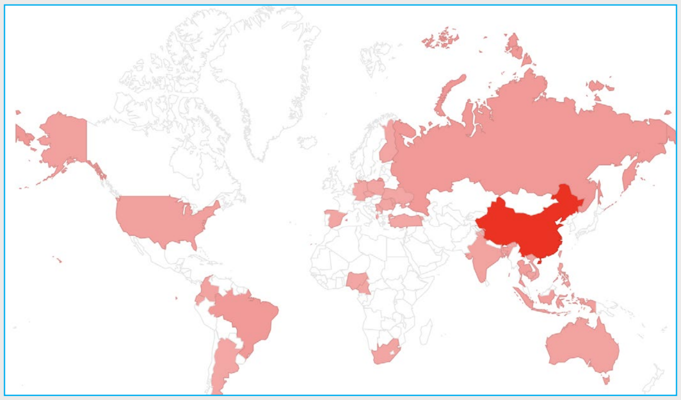
■ ***Figure 1:*** *Authentication Attempts During a 7-day Period with Timing of Each Wave Highlighted.*

The First Wave

We began investigating this bad actor after we noticed a surge in traffic attempting to authenticate. The traffic was detected as non-human and subsequently stopped.

During this first wave, the attacker used two evasion techniques:

1. **A worldwide proxy network**
   - The attacker rotated IPs for every request (see Figure 2).
   - This technique bypasses mechanisms that cannot detect malicious requests on the first page load.
2. **Browser session hijacking**
   - The attacker used a legitimate browser session that had been established with the website.
   - This technique enables the attacker to bypass detections that rely on trusting pre-established browser sessions.



■ ***Figure 2:*** *Geographic Locations of IPs Used in the Initial Wave.*

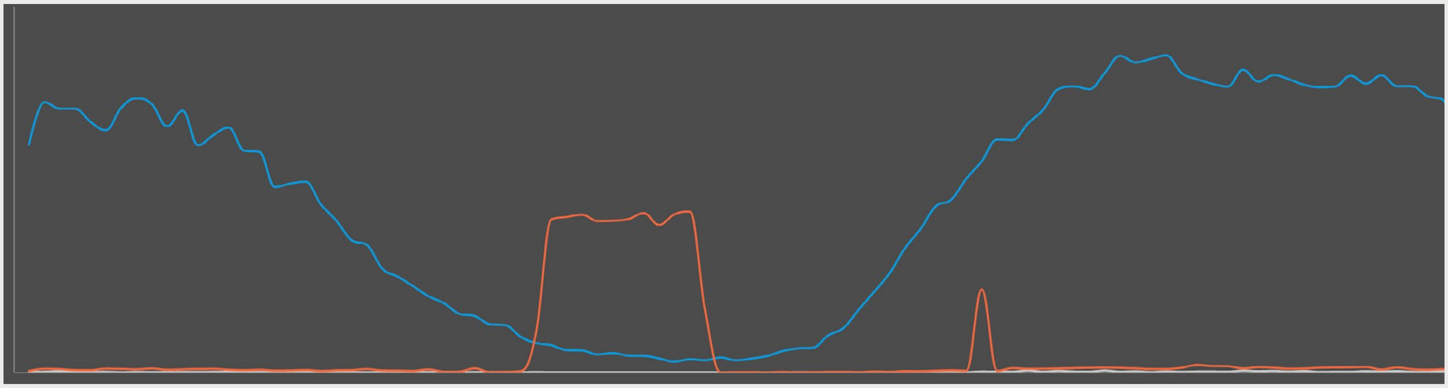
This wave lasted for less than an hour, which indicates that the attacker was monitoring the attack very closely. As soon as they realized their efforts were not successful, the attack was stopped to avoid the risk of unwanted attention.

The Second Wave

Within 72 hours of the initial failed wave, the attacker returned in full force. After revising the failed evasion techniques from the first wave, the attacker came back with the next evolution:

1. **Localized residential IPs**
   - The attacker shifted away from using a worldwide proxy network and focused on ensuring that traffic came from the correct geographical location.
   - This enables an attacker to blend in more effectively with legitimate customer traffic hitting the application.
2. **Clean browser sessions**
   - Instead of re-using a browser session, the attacker attempted to create new, clean sessions with each authentication attempt.
   - This technique enables attackers to bypass detections that rely on profiling browsers over a number of requests before making a decision.

This wave lasted longer than the first, however none of the attacker's authentication attempts were successful. After a number of hours recycling these techniques, the attacker gave up (see Figure 3 below).

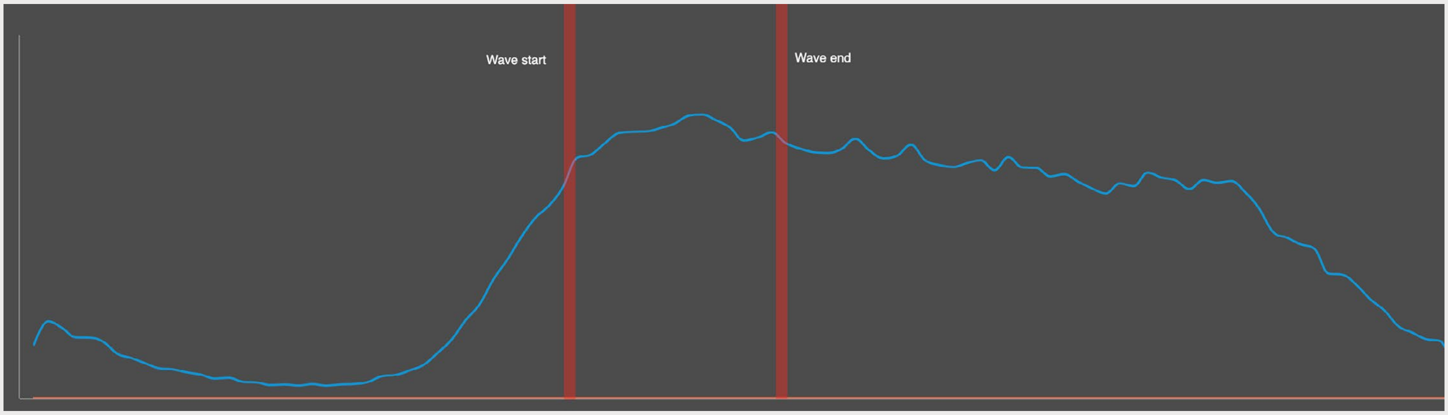


■ ***Figure 3:*** *Authentication Traffic Over a 24-Hour Period, With Attack in the Middle of the Night, Local Time.*

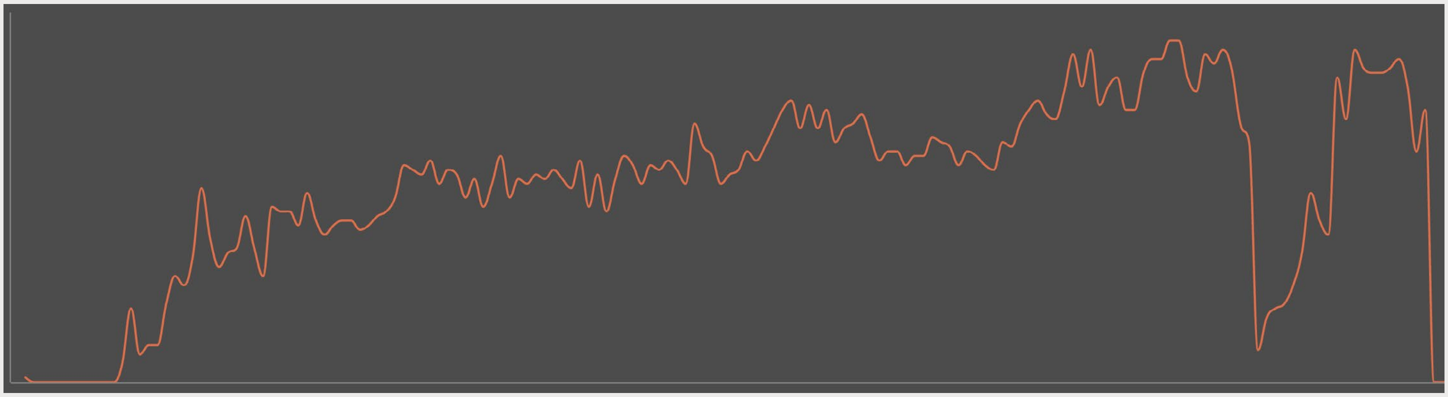
The Third Wave

The third and final attempt came 24 hours after the second one. This wave used the two techniques from the second wave, with a new shift in behavior: Mimicking the timing of legitimate user traffic.

In the attacker's two previous attempts, attacks were launched during the middle of the night for the majority of this organization's typical customers. This time, the attacker used the localized IPs and new browser sessions and started the attack slowly, as customers in that region started to wake up (see Figures 4 and 5, below).



■ ***Figure 4:*** *All Authentication Attempts Processed During Final Wave.*



■ ***Figure 5:*** *Final Wave Ramp-up Over 3 Hours to Mimic Legitimate Customer Traffic Patterns.*

Uncovering the Reconnaissance Period

Using Kasada's sophisticated browser-sensor interrogation, session tracking, and data analytics tools, we worked backwards from these three attacks to isolate the reconnaissance traffic from the attacker before the actual attack began.

The reconnaissance period lasted roughly one hour, during which time more than 12,000 legitimate customers logged into the application. Our attacker was simply a needle in a haystack at this point (see Figure 6).

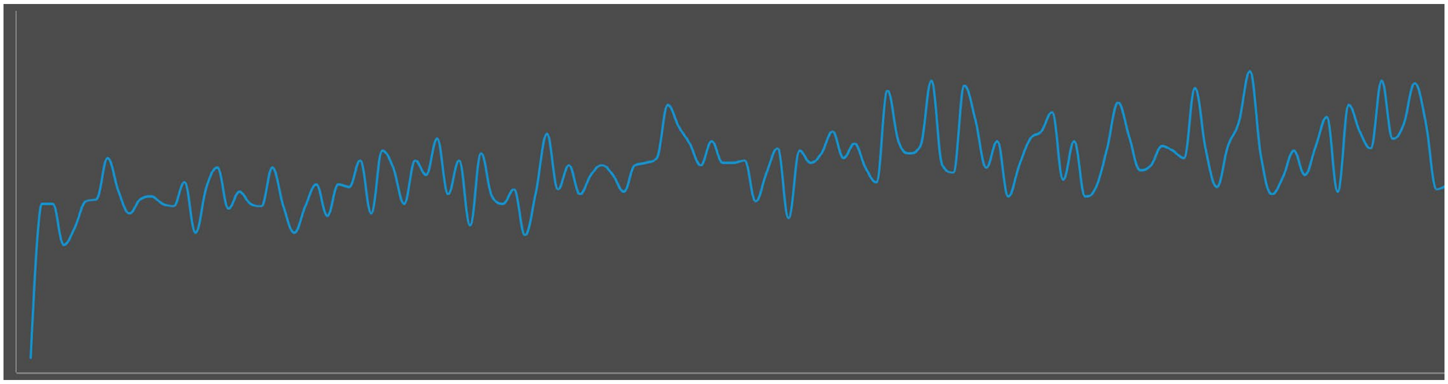


Figure 6: *Legitimate Users During Reconnaissance Period*

After correlating a number of key characteristics, we identified the browser from which the attacker first started testing. This is how the attacker conducted reconnaissance (see Figure 7):

1. Load the customer application in a browser
2. Test two logins
3. Transfer the browser session into a bot to test logins
4. Refresh browser and continue debugging bot

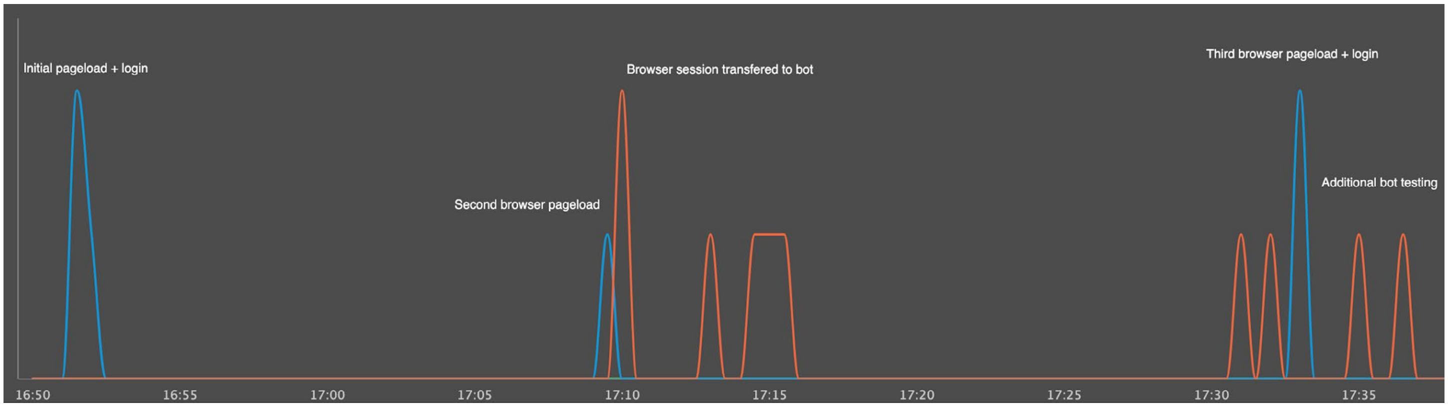


Figure 7: *Tracking the Reconnaissance Period*

Final Observations

During each stage, the attacker used various methods of evasion in different combinations. Because the attacker was unable to reverse-engineer and understand the detections in place at this retailer, he or she incorrectly made the assumption that simple techniques might work to bypass WAFs or other bot detection solutions in this scenario.

Ultimately the attack was unsuccessful because of the defense in depth that the retailer had in place, which thwarted all of the various methods the attacker used to evade detection. Had the retail brand not implemented a layered security solution, the attacker would have most likely been successful earlier in the attack and inflicted significant damage to the company.

layered security solution, the attacker would have most likely been successful earlier in the attack and inflicted significant damage to the company.

In this attack, Kasada's multiple layers aided in detecting the various techniques that this actor used. This was also key to automatically handling the retooling attempts, as our platform remained one step ahead of what the attacker was doing, without requiring any human intervention.

The high level of visibility that Kasada provides into application traffic is critical to identifying and isolating attack traffic even when it is a needle in a haystack. With these actionable insights, we can create highly accurate and specific indicators of compromise (IOCs) to share with our customers, ensuring that they'll be able to proactively stop attacks like this one if this group visits any of their applications.

How Kasada Can Help

Kasada is a modern bot mitigation solution that protects your company against the damaging, often underestimated effects of malicious automation across your web, mobile, and APIs. Kasada offers a cloud-based service that puts no extra maintenance or burden on your internal team.

Unlike alternative solutions that provide incomplete, easy-to-detect, and inefficient bot mitigation tools (which are not only costly to deploy and maintain but also add friction and latency to the user experience), Kasada:

- Looks for immutable evidence of automation from the very first request, instead of relying on contextual data from the past which takes time and ongoing maintenance.
- Makes bots, not humans, do the work, by cleverly deterring synthetic traffic with a cryptographic challenge that makes it arduous and expensive for bots to continue their attacks, while remaining imperceptible to (and requiring no action from) end users.
- Is extremely efficient, easily implements within minutes, and demonstrates clear ROI across multiple departments.
- Is highly effective, delivering the best detection and lowest false positive rates in the market today.

How Kasada Works

Using proprietary techniques, Kasada presents a myriad of obstacles to frustrate and disrupt the operating model of bot attacks, preventing hackers from using automation and challenging critical aspects of the attack process.

When bots that are imitating human users interactwith your application, they leave certain traces of automation within the client environment. Kasada's invisible client interrogation process, with advanced JavaScript inspection processes, detects the presence of such traces and uses the telemetry in our decision engine to detect and stop attacks. This immediately detects bots and categorizes them as benign or malicious. This interrogation process is invisible to normal users and doesn't require the use of CAPTCHAs, which have been shown to be ineffective in evading malicious bots. Kasada's world-class obfuscation enables long-term efficacy.

A cryptographic browser-based challenge is used as aproof of work that exponentially increases the difficulty level with the number of abusive requests over time, therefore exhausting the CPU resources of bad bots, without informing the adversary. This forces the attack to permanently cease, as its ROI inevitably collapses. Notonly does Kasada neutralize the attack long-term, but also prevents the bot operator from quickly retooling or attacking other targets, as all CPU resources have been exhausted. Fraudsters then avoid targeting Kasadaprotected properties, as it costs them virtually unlimited resources to try and break in.

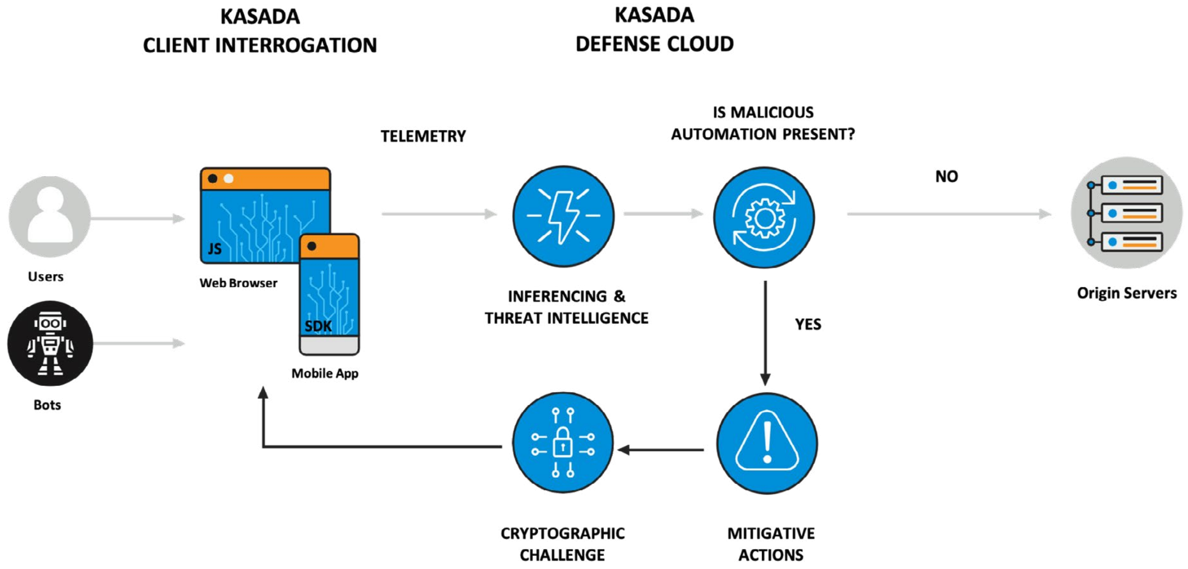


Figure 8: *How Kasada Works*

Primary Use Cases

Kasada efficiently and effectively combats automated threats and bot-drivenfraud, including login fraud, scraping fraud, and financial fraud:

- Credential stuffing
- Fake account creation
- Carding, checking, and skimming
- Denial of inventory
- Service disruption and application denial of service
- Content scraping
- Competitive data scraping
- API scraping
- Ticket scalping

Customer Testimonials

“Kasada was implemented in just minutes, and immediately neutralized our flow of attacks. Amazed by how simple and immediately efficient the solution was, we also really liked the interaction with the Kasada team. They were enthusiastic, highly knowledgeable and very easy to do business with”.

— Regan MacDonald, Group IT Manager, True Allianc

“The entire team was so amazed; we had never seen such fast, immediate ROI on a security tool. In just under 30 minutes, we set-up, turned on, and stopped the attack. It was an out-of-the-box experience with instant results. Kasada is a partner that has overdelivered.”

— Nik Pinchuk, VP Global Engineering, PointsBet

Benefits of Using Kasada

Kasada is leading the fight with novel approaches and cloud-based technology to detect and mitigate the maelstrom of malicious traffic that other security platforms can’t:

Immediate Time-to-Value

- Onboards and provides time-to-value in 30 minutes
- Inexpensive to install and manage: cloud-based, no hardware required
- Little to no maintenance needed

Long-Term Efficacy

- Offers world-class obfuscation
- Stops bad bots on the first request, including new bots, and provides continuous mitigation
- Remains effective by frustrating fraudsters and fighting back

Frictionless Customer Experience

- Invisible to end users, eliminating the need for CAPTCHAs
- Virtually zero false negatives and 0.001% false positives
- CDN-agnostic and complements existing fraud solutions

Business Visibility

- Completely removes malicious bot traffic, enabling accurate web metrics
- Actionable insights into human, good bot and bad bot traffic
- 24/7/365 support

To learn how Kasada can help your business defeat automated attacks, request a demo today.

About Kasada
Kasada is the most effective and easiest way to defend against advanced persistent bot attacks across web, mobile, and API channels. With Kasada, trust in the Internet is restored by foiling even the stealthiest cyber threats, from credential stuffing to data scraping. The solution invisibly stops automated threats while inflicting financial damage to attackers, destroying their ROI. With the ability to onboard based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, please visit www.kasada.io and follow on Twitter, LinkedIn, and Facebook.

For more information, visit www.kasada.io.