Online Retail Threats

Credential Stuffing

Online retailers must deliver a compelling user experience across web and mobile channels while protecting customers from cyberattacks and fraud. This report looks at one of the most common threats to retailers - credential stuffing - and how Shape works with major retailers to shut these attacks down.

SHAPE

Contents

> **"A breach anywhere is a breach everywhere."**
>
> Shuman Ghosemajumder | CTO, Shape Security

Credential Stuffing

Automated Attacks

Online credentials have been stolen and compromised for almost as long as the Internet has existed. But in the past decade, the frequency of credential theft has increased and the tools and techniques used by cybercriminals have evolved.

Today, usernames and passwords act as keys to online services that are vital to many aspects of people's lives such as their retail, banking, travel, and insurance accounts. And yet, those accounts are less secure than they have ever been, due to the scale and scope of data breaches on unrelated sites.

Theft of user credentials has ramped up significantly for a number of reasons. First, users are reusing the same usernames and passwords across multiple sites. Second, automated tools can take stolen credentials and test them on other sites at a massive scale. And third - and perhaps most important - many customers have high value assets, from PII to loyalty points to stored credit cards and gift cards, that are extremely lucrative targets for cyberattacks.

Credential stuffing, first recognized in 2011, is now the single largest source of account takeover and automated fraud on most online services. It's the large scale, automated testing of stolen usernames and passwords against a range of online sites. What's particularly challenging is that this threat doesn't exploit an accidental vulnerability in an application. Instead, it exploits intended functionality - the login form where anyone could enter the right credentials to access an account, its data and privileges. The other challenge is that your site may not have been compromised, but usernames and passwords stolen from another site are now being tested on your site to gain access.

This means that there isn't a simple "defect" to fix, or patch to issue. Instead, the defense of a login application against automation and the exploitation of spilled credentials is a much more difficult and complex challenge, extending into user behavior (password reuse) and poor security practices at third-party sites.

- Credential stuffing is now responsible for more than 99% of all retail account takeovers (ATOs).
- Shape observes over 90% of login requests on many of the world's largest web and mobile applications coming from credential stuffing.
- Shape observes typical success rates of 0.1% to 2% when stolen credentials from one site are used by cybercriminals to log into and take over accounts on other sites.
- Shape regularly detects Sentry MBA in particular being used for attacks against nearly every customer in every industry.

But First, The Credential Spill

A credential spill occurs when user credential data, like usernames and passwords, are stolen from an organization or its users. "Spill" refers to the fact that stolen credentials do not just affect the company which was originally hacked or breached, but are now available for use in attacking any other website or mobile application.

"The problem was with other websites," explained one Fortune 100 retailer's CISO. "Our customers reuse the same passwords across multiple sites. When other sites get breached, fraudsters use those spilled credentials to hijack my customers' accounts."

"Account checkers: Cybercriminals engaged in mass-compromise of accounts, such as those who sell accounts on the Slilpp marketplace, likely employ customized multi-site account checkers that are constantly updated to circumvent new defenses put in place by target organizations. Account checkers run leaked credentials against online customer accounts. In some cases, we identified a spike in the number of a specific organization's accounts available for sale by individual sellers, then a temporary lull in the number of accounts added, followed by another spike of the same accounts from the same seller. This suggests that as retailers may modify or enhance their customer account security, criminals using account checkers experience temporary lulls in inventory as they update their tools to circumvent the new defensive measures."

Booz Allen Cyber4Sight Special Report - 2017 Peak Retail Season

Note that the industries targeted for credential spills, such as gaming, are often different than the industries then targeted with the stolen credentials. Retail is a popular target.

Why Retail Is A Popular Target

Credential stuffing against retail web properties is especially lucrative, for a number of reasons.

90% **of login traffic on many of the largest retail websites is automated**

First, retail websites are designed to cause as little friction for customers as possible so security is often sacrificed for user experience. For example, in a crime-free world retailers would prefer to dispense with CAPTCHAs, two-factor authentication, and excessive emails or texts confirming every change to an account. In fact, many retail sites keep users logged in to make "continue shopping" even easier. In contrast, financial services providers, for example, never allow this to happen, automatically logging a user off after 10-15 minutes of inactivity.

Second, attacking retail websites can also be lucrative because there are typically more opportunities to monetize illicit account access than with any other vertical. Attackers can steal personal data, exploit saved credit cards and gift cards, or sell the whole account on the Dark Web for use by criminal organizations. Automated attacks against retailers can also facilitate more traditional offline fraud such as return fraud or the theft of goods.

How to Spot a Credential Stuffing Attack

Most retailers have no visibility into, or even awareness of, the volume of automated login traffic they are experiencing from credential stuffing attacks.

As we said, credential stuffing attacks appear as legitimate requests to the security controls in place on most applications. Since real user credentials are being used, these types of attacks do not need to use brute force techniques to attempt to guess passwords. Instead, they just need to "behave" the way a legitimate user would, providing their own credentials. So when the process is fully automated, credential stuffing attacks can achieve incredible scale and efficiency.

What a detection solution will see is that a vast majority of traffic is actually automated, coming from cybercriminals testing stolen credentials rather than from the site's legitimate users accessing their accounts in a manual fashion.

Other signs a credential stuffing attack is underway:

- The volume of attempted logins will be far higher than usual, and also spread over 24 hours versus daytime and evenings when most consumers shop.
- A low login success rate from a specific number of IPs, autonomous system numbers (ASNs), or user agents (UAs), although this becomes more difficult to see as attacks become more distributed.
- Users who do not generate any keystrokes or mouse movements. This also becomes more difficult to spot as attackers start using more advanced tools to generate human-like interactions.
- Pay particular attention to virtual hosting ASNs, such as AWS, Digital Ocean, Claro S.A., and Choopa, LLC.
- Look for the default UAs and ASNs used by Sentry MBA. (More details can be found here at our 2017 Credential Stuffing report.)

Credential Stuffing In Action

Let's take a closer look at some examples of a major retailer dealing with a credential stuffing attack.

Figure 1 shows actual incoming login traffic for one of Shape's Fortune 100 retail customers. More than 92% of the incoming login traffic for this customer was from automated credential stuffing, shown in yellow. Red is where Shape beings blocking the logins. Green are the real human logins.

In the first several days, Shape was able to distinguish between real human user traffic (green) and automated credential stuffing traffic (yellow). Once Shape went into blocking mode, the automated traffic was blocked (red) and was no longer successful at login, and after a few more days, the cybercriminals moved on to other targets.

For this customer, more than 92% of their incoming login traffic was from credential stuffing attacks which bypassed their industry standard security controls. This large amount of automated traffic placed a heavy load and cost on infrastructure, added login latency for real users and skewed website traffic analytics creating wasted marketing spend.

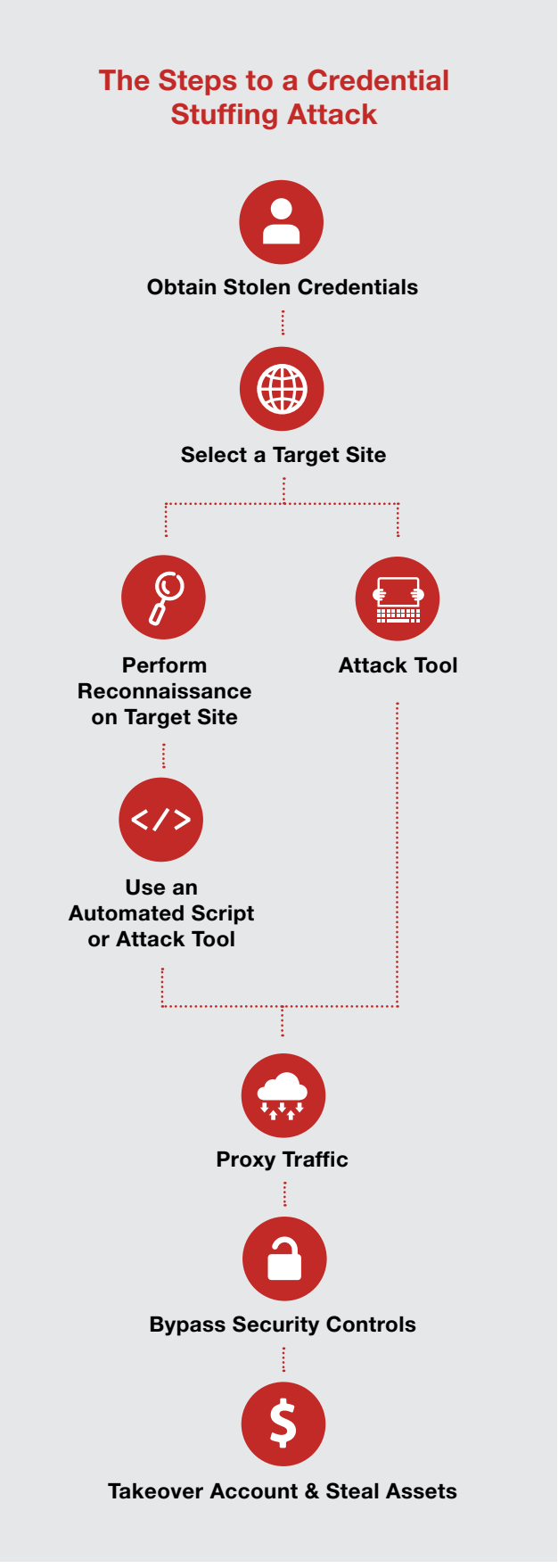
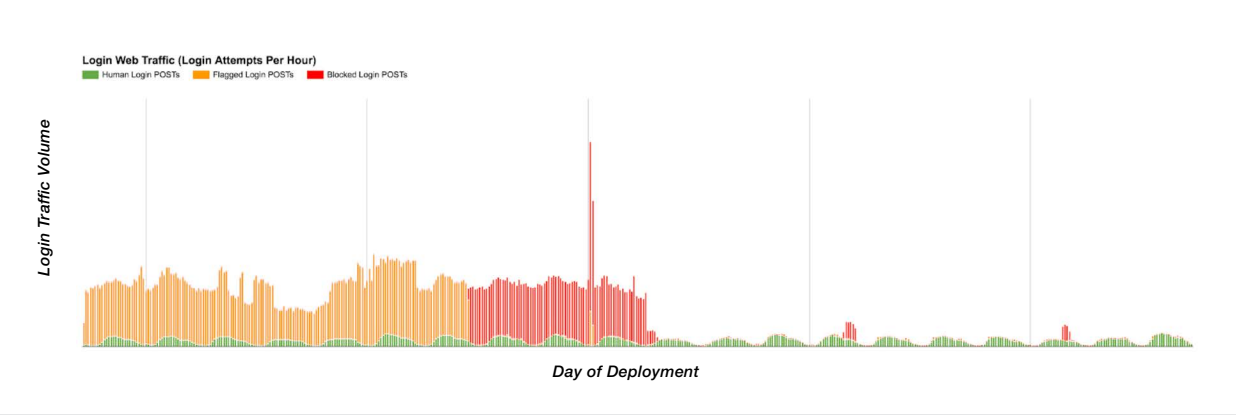


Figure 1

Incoming Automated and Legitimate Customer Login Traffic for Shape Customer



In another example with a Fortune 500 retailer, Shape observed over 15.5 million account login attempts during a four month period, and identified that over 500,000 accounts were on spilled credential lists. Shape tracks credentials actively being exploited across the Shape network, previously used in actual credential stuffing attacks.

Shape analyzed a sample of six billion login and search page submissions over a one month period.

In two days, the retailer saw two major attacks with over 20,000 total login attempts. During one day, the retailer witnessed over 10,000 login attempts from over 1,000 IPs.

Two attacks highlight how cybercriminals are turning their attention to mobile APIs. The first attack focused on the target's traditional web application and made over 30,000 login attempts using proxies located in eastern Europe. The second attack focused on the target's mobile API and made over 10,000 login attempts on a daily basis. We usually see no more than a 30 day period once Web endpoints have been mitigated before the attacks move on to the mobile site. Both attacks shared hundreds of IP addresses and other characteristics, indicating the same actors may have been responsible. These type of highly distributed attacks bypass typical security such as WAFs since the individual attack volume from any specific IP address is less than the threshold most WAFs are set to detect.

80K	3.7K	1.8K
IPs	ASNs	UAs

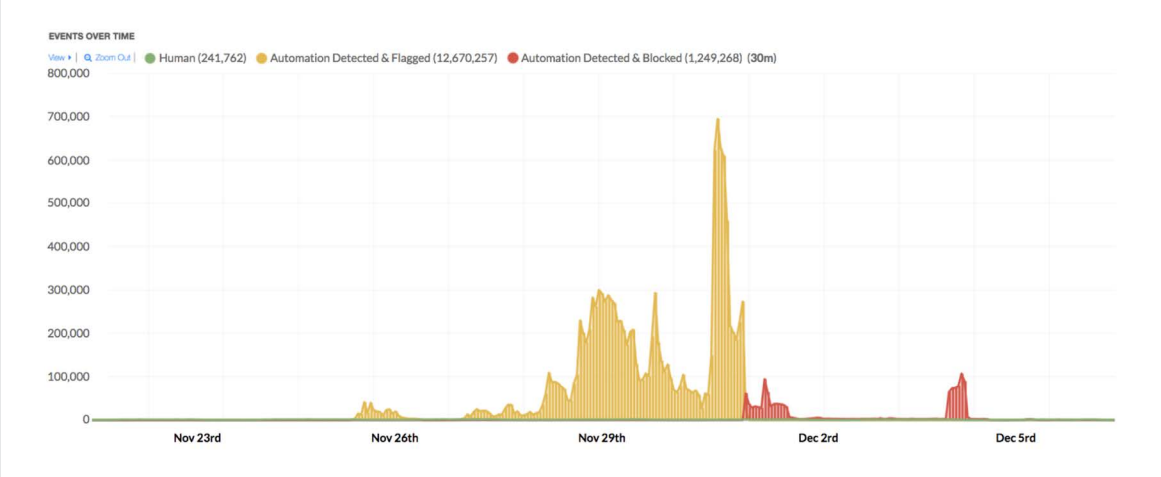
This contrasts to traditional attacks where we would see just a few IPs driving a lot of traffic.

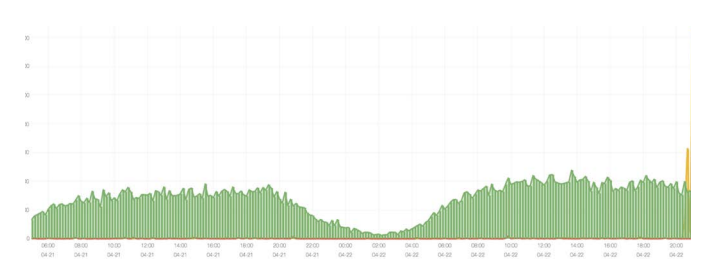
The diagram below (Figure 2) illustrates the traffic during one attack over a ten day period.

Yellow is monitored traffic and red represents detected traffic (note - the green line is actual human traffic, showing how large scale the attack is compared to normal traffic). One interesting characteristic with the green traffic - being human - is that it's mostly during the day. Note how the yellow traffic is ongoing 24 hours - reflecting its automated nature. Automated attacks don't sleep.

Figure 2

Shape Security in Action over 10 Day Period with a Major Retailer





On December 1, the yellow turns to red as Shape turns on blocking mode. Every 30 minutes Shape observes 1.4m automated attacks.

Then on December 5 the red spike returns - the attacker has regrouped and retooled and is trying again. But this attempt fails and they give up.

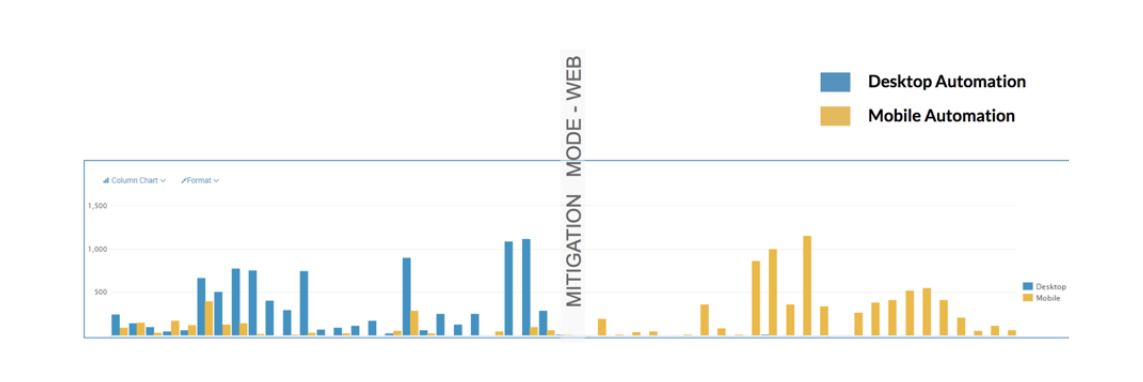
Also important to note - this attack is happening over the critical Black Monday through early holiday season shopping period. Again, an important time for any major retailer to be performing flawlessly for real customers.

Following a successful initial deployment, the Fortune 500 retailer rolled Shape out to protect additional web applications and API services used by mobile applications (Figure 3 below). The retailer has eliminated tens of millions of dollars in fraudulent transactions and chargeback fees. The retailer also benefits on an ongoing basis from threat intelligence (collected and correlated across all Shape deployments) and consultation provided by Shape's anti-automation experts to stay ahead of cybercriminals.

"The Shape team worked with my team to go live in two weeks from start to finish. Unlike traditional security solutions, we don't need more training or headcount to get value out of Shape's solution. They've completely blocked the attackers without inconveniencing my users or imposing on my team."

Fortune 500 Retailer CISO

Figure 3



This graph shows only the automated traffic. Initially the automated traffic is coming through the website (blue). Once Shape starts blocking or mitigating the web, the automated traffic shifts almost right away to the mobile channel.

Increasingly Sophisticated Attacks

But credential stuffing attacks are getting only more sophisticated. In particular, we're seeing:

1. Highly distributed infrastructures
2. Omnichannel attacks, moving from a website to mobile
3. Increasingly sophisticated tools, for example, executing the JavaScript, rendering a real browser, imitating user fingerprints and mouse movements, etc.

Why Retail Customers Choose Shape

Shape is committed to helping protect retailers from the threat of credential stuffing attacks, by detecting and stopping automated logins and other fraud, and making it economically unattractive for cybercriminals to continue their attacks.

- Shape retail customers account for over $75 billion in annual online revenue
- Shape protects 40 million retail end-users from credential stuffing and account takeover
- Shape protects nearly 800 million transactions per week for retailers

Shape Data Network

By working with major online properties across top industries - retail, financial services, travel and hospitality to name a few - Shape has created the Shape Data Network. It benefits all of our customers because when one property experiences credential stuffing we can immediately alert and protect all other properties, regardless of industry.

Shape Enterprise Defense determines in real-time if an application request is from a fraudulent source and then takes an enterprise-specified action, such as blocking, redirecting, or flagging the request.

Blackfish is an artificial intelligence system to identify passwords stolen from data breaches that have not yet been discovered or disclosed, and whose data is not on the dark web.

For more, view our Credential Stuffing Threats and Retail Case Studies

www.shapesecurity.com
1-650-399-0400

General Inquiries
info@shapesecurity.com

Sales Inquiries
sales@shapesecurity.com

Press Inquiries
press@shapesecurity.com