HUMAN

HUMAN Sightline Cyberfraud Defense Case Study

Top E-Commerce Retailer Prevents Credential Stuffing with HUMAN

Company

This e-commerce retailer is one of the **world's largest sellers** of photo, video, audio and computer technology. Millions of audio and imaging professionals rely on its products to power their creative pursuits.

Challenge

This large e-commerce retailer was bombarded with credential stuffing attacks that led to account takeovers (ATOs). Its bandwidth was saturated with malicious traffic, and successful attacks resulted in chargebacks and other fraud that resulted in financial losses, customer churn and brand reputation damage.

Solution

The retailer implemented HUMAN Sightline to detect and mitigate malicious bots across its e-commerce website. The solution solves for full-fledged ATO attacks in real-time, and stops fraudsters using compromised credentials on websites and mobile apps.

HUMAN Sightline leverages an expansive, dynamic and up-to-date database of compromised credentials that HUMAN gathers from its unmatched visibility into the internet. The HUMAN platform verifies the humanity of **15 trillion interactions each week and sees 3 billion each day**. This allows us to zero in on compromised credentials that are actively in use, rather than an outdated list of credentials stolen in past breaches.

Results

HUMAN Sightline provides an early signal that cybercriminals are attempting to log in with stolen usernames and passwords. This enables the retailer to take mitigating actions ahead of ATO attacks, such as notifying users that their credentials have been breached and triggering a password reset. This yielded a number of results:

REDUCED CREDENTIAL STUFFING ATTACKS

Following the deployment of the solution, the e-commerce retailer realized a **more than 90% reduction in the magnitude of credential stuffing attacks**, and the number of accounts at risk of ATO dropped from **nearly 2.5 million per quarter to less than 2,500**.

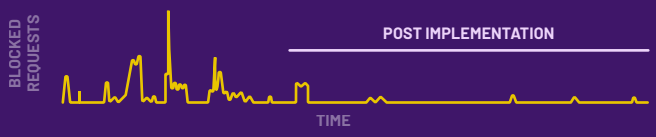


Figure 1 shows the volume of credential stuffing attack attempts before and after implementation of the solution.

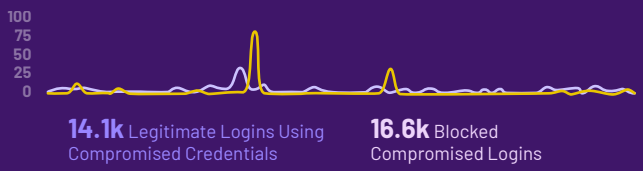
DECREASED NUMBER OF ACCOUNTS AT RISK OF ATO

In the first two weeks alone, **HUMAN identified 3,988 login requests** using compromised credentials. The solutions blocked these login requests and prompted users to change their passwords.

Figure 2 shows the reduction in accounts using compromised credentials over time.

SERVED AS AN EARLY WARNING SYSTEM

Attackers sometimes conduct a dry run with manual attempts before launching the full bot attack. The graph to the right shows an example in which the solution flagged some of the manual logins (teal line), acting as an early signal that a larger scale attack was coming (purple line).



Takeaway

HUMAN Sightline works because of HUMAN's unparalleled visibility into what's happening online. We leverage information gathered from every digital interaction we observe to build our credential database. By stopping the use of these stolen credentials up front, the solution prevents fraud before it happens. This decreases fraud claims, transaction fees and write-offs, protects brand reputation and instills trust in consumers that their accounts are safe on your site.

HUMAN identified 3,988 login requests using compromised credentials in the first two weeks.

After implementing HUMAN, the e-commerce retailer saw a more than 90% reduction in credential stuffing attacks.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit ***www.humansecurity.com***