Protecting a Stock Photography Website Against Credential Stuffing and Account Abuse Bots

NETACEA

Protecting a Stock Photography Website Against Credential Stuffing and Account Abuse Bots

THE CHALLENGE | THE SOLUTION | THE OUTCOME

CUSTOMER PROFILE

- Stock photo provider with a library of hundreds of millions of images and videos
- High-quality media assets licensed from over one million contributors
- Operating globally with revenue in the hundreds of millions

RESULTS

- Malicious traffic reduced by 97%
- Resale of accounts on the dark web blocked, with reports of stolen accounts reduced by 98%
- Credential stuffing attacks detected and averted with very low false positive rate
- Identified sophisticated bots that WAF alone was less than 50% effective at recognizing

THE CHALLENGE

The client is a licenser of stock photography, used by businesses and enterprises across the world. The hundreds of millions of images it offers to individual customers and businesses of all sizes are sourced from over one million contributors, who receive a fee each time their content is licensed.

With such a vast library of media assets available via account subscriptions and pay-per-asset models, it's unsurprising that criminals were targeting the site's accounts.

Exploratory work by our dedicated Threat Research team confirmed that the website's assets frequently featured on the dark web, with lifetime premium account access and packs of stolen images available to purchase at a fraction of their usual cost.

This was the result of bad actors using credential stuffing bots to bombard login pages with stolen credentials, gaining unauthorized account access wherever they found a match.

The fraudsters weren't just targeting customer accounts. They were also going after valuable contributor accounts. These accounts were prime targets for account takeover (ATO) as they contain monetary balances earned through licensing assets to the website's customers.

The anatomy of credential stuffing and account takeover attacks

Step 1 – Credential acquisition

Whenever a company's customer data is leaked on the internet, criminals can use the login credentials to attack other websites. Criminals exploit the common tendency to reuse username and password pairs across multiple services. If passwords are absent or encrypted, adversaries instead use lists of commonly used passwords to crack accounts by brute force.

Step 2 – Credential stuffing

Criminals then attempt to use their list of full or partial credentials to gain access to other sites. This is done automatically in huge volumes using credential stuffing bots, which can submit hundreds of login attempts in a short space of time and validate working credentials instantly.

Step 3 – Account takeover

With a list of validated login details, attackers can gain access and lock the rightful account owner out. This can be done automatically with bots, either as soon as an account is validated or later to evade suspicion. It can take hours, days, or weeks for the rightful account owner to notice, by which time their credits are cleaned out. The website then loses money in reimbursing the lost credits and wastes resources by investigating and repatriating the stolen account.

Step 4 – Reselling and profit making

Criminals put stolen accounts up for sale on the dark web, drastically undercutting the original subscription price. The victim business loses out on subscription sales, and the bot operator makes a profit for very little effort or investment.

ABOUT NETACEA

Netacea provides an innovative bot management solution that solves the complex problem of credential stuffing, account takeover and other malicious bot activity for our customers in a scalable, agile and intelligent manner, across websites, mobile apps and APIs.

Our Intent Analytics® engine is driven by machine learning to provide an in-depth analysis into all traffic on your site. This gives us an incredibly fast and comprehensive understanding of human and automated traffic behavior, enabling us to identify and block bots in real time with unparalleled accuracy.

With machine learning at the heart of our approach, our technology provides an innovative and profoundly effective solution that is configurable to your environment and adapts to changing threats.

FREE TRIAL

Find out how Netacea's unique approach to bot management can help your business keep bad bots at bay. Get a personalized demo of Netacea Bot Management for your business and get control over your website traffic.

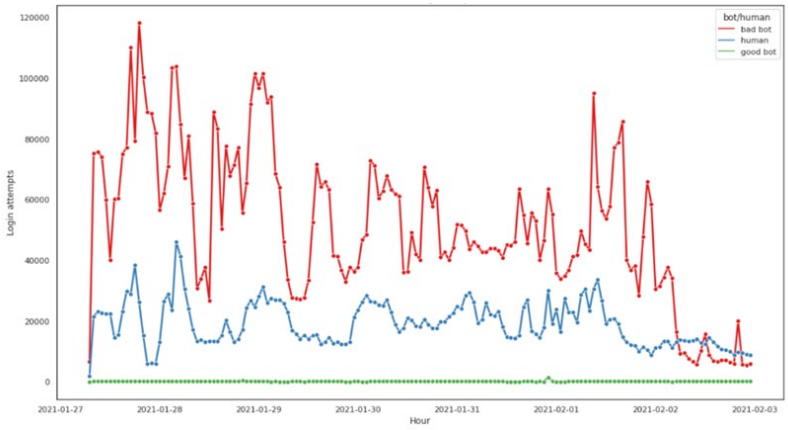
THE SOLUTION

Netacea Bot Management was integrated with the client's website, gaining full visibility of traffic across all areas of its web estate.

Netacea's Intent Analytics® machine learning engine and team of Bot Experts analyzed traffic across the whole domain. This quickly confirmed that 70% of the traffic on the user accounts area of the site was automated – in other words, most of this traffic came from bots alone.

Furthermore, only 40% of the traffic on the contributor section of the site was identified as 'human', with highly distributed bot traffic consistently infiltrating the site throughout the week.

Analysis of the behavior of this bot traffic confirmed that its intent was a malicious combination of credential stuffing and account takeover attacks on several login pages.



Although the client has a web application firewall (WAF) in place to block malicious traffic, it was only able to stop less than half the bots identified by Netacea Bot Management.

THE OUTCOME

By identifying anomalous behavior and its origins, Netacea Bot Management advised blocking bad bots before they reached the client's web servers.

Attack overview

- 2.3 million malicious login attempts in 48 hours
- 100% CAPTCHA incomplete rate on blocked user agent
- Very low false positive rate on blocking action

In one instance, blocking a single user agent prevented 2.3 million malicious login attempts over a 48-hour period, shutting down a sustained credential stuffing attack with almost zero false positives – meaning no impact on genuine customers.

This was a high-volume credential stuffing attack, where the threat actor was using bots disguised as human and distributed across over ten different countries to confirm the validity of stolen credentials on the client's login page, so they could access these accounts later to strip out any useful data and assets or sell them on the dark web.

However, we were able to block 98% of the requests before they could validate any user account credentials.

As a result, threat actors' ability to acquire and sell premium accounts has been drastically weakened, with reports of fraudulent account access dropping by 98%. Blocking 97% of malicious traffic overall has also reduced server load, meaning the client can spend less on IT infrastructure and more on other areas of the business.