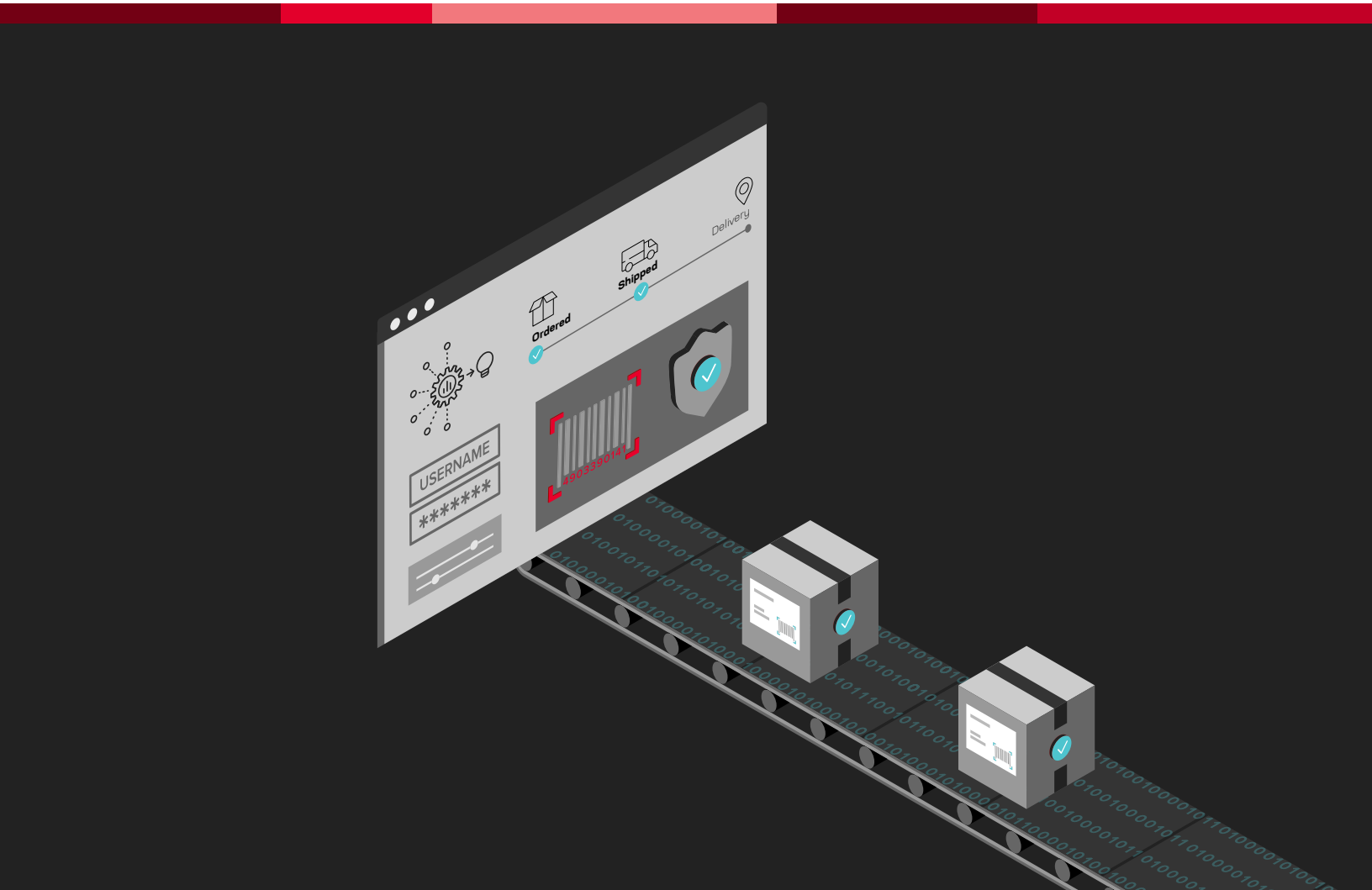
CASE STUDY

Courier Prevents Shipping Fraud



ATTACK TRAFFIC WAS MORE THAN 100,000 POSTS IN A SINGLE DAY

The Customer: Top 5 Courier. A top 5 global courier ("provider") with over $50 billion in annual revenue wanted to protect its customers from account takeover and prevent fraudulent account creation.

Challenge 1: Account Takeover

The provider wanted to protect customer logins on its web and mobile applications from credential stuffing attacks. Credential stuffing is an attack in which criminals test credentials stolen from third parties en masse on login applications to commit account takeover. Attackers obtain a large list of stolen credentials and typically find about 0.1% to 2% of the list is valid on a target site because users reuse passwords.

Over an eight month period, the provider experienced three separate waves of large volume automation spikes in addition to sustained automated traffic. In some cases, attack traffic was more than 100,000 POSTs in a single day, which was a 50% spike over legitimate traffic. The provider also released a major native mobile API upgrade in the fall of 2017, which was frequently targeted by attackers.

The attacks were costly to the provider, which had to reimburse the funds stolen from its customers as well as any chargeback fees from unauthorized transactions made using a credit card linked to the account. Even the credential stuffing attacks themselves were costly for the provider. Customers would flood the help desk with complaints about missing packages or their accounts being locked (which occurred due to excessive failed login attempts from an attacker).

Challenge 2: Fraudulent Account Creation

The provider also faced a challenge with two different schemes based on fraudulent account creation. In the first scheme, criminals programmatically created fake accounts using addresses in affluent zip codes, correctly answering the knowledge-based authentication questions using publicly available personal data. They then used the provider's free service to track packages and receive notifications when packages shipped. This enabled thieves to track packages and intercept shipments, many of which included goods they could resell.

In the second scheme, attackers created fake accounts and attached stolen credit cards to them. They then advertised services such as discounted shipping and package forwarding on illegitimate marketplaces, using the fake accounts to purchase shipping labels. If and when the credit card theft victim discovered the fraud, the courier would have to refund them the cost of shipping as well as possibly pay chargeback fees to the credit card issuer.

WHY F5?

F5 Distributed Cloud Bot Defense was selected for three key reasons:

1. Long-term efficacy in blocking sophisticated attackers and capability to identify malicious activity leading to fraud.
2. Omni-channel protection including web, mobile, and API endpoints.
3. Fully managed service that became an extension of the provider's security team and focused on delivering its desired outcome: stop all unwanted automation.

The Solution

The provider first attempted to build its own solution to address these challenges. It used a combination of a web application firewall, load balancer and analytics tools to try to solve the problem by correlating help desk tickets with customer complaints and then forcing a password reset. This DIY approach was not effective in mitigating the automated attacks, and the fraud persisted.

Unable to solve the problem on its own, the provider turned to F5® Distributed Cloud Bot Defense, and decided to deploy the solution across its login and account creation applications on both web and mobile.

The Outcome

There are two stages to a typical Distributed Cloud Bot Defense deployment: observation mode and mitigation mode. In observation mode, F5 analyzes all incoming requests to the application in order to customize its defense and flag automated traffic. In mitigation mode, F5 takes programmatic action based on the nature of the automation and the provider's needs.

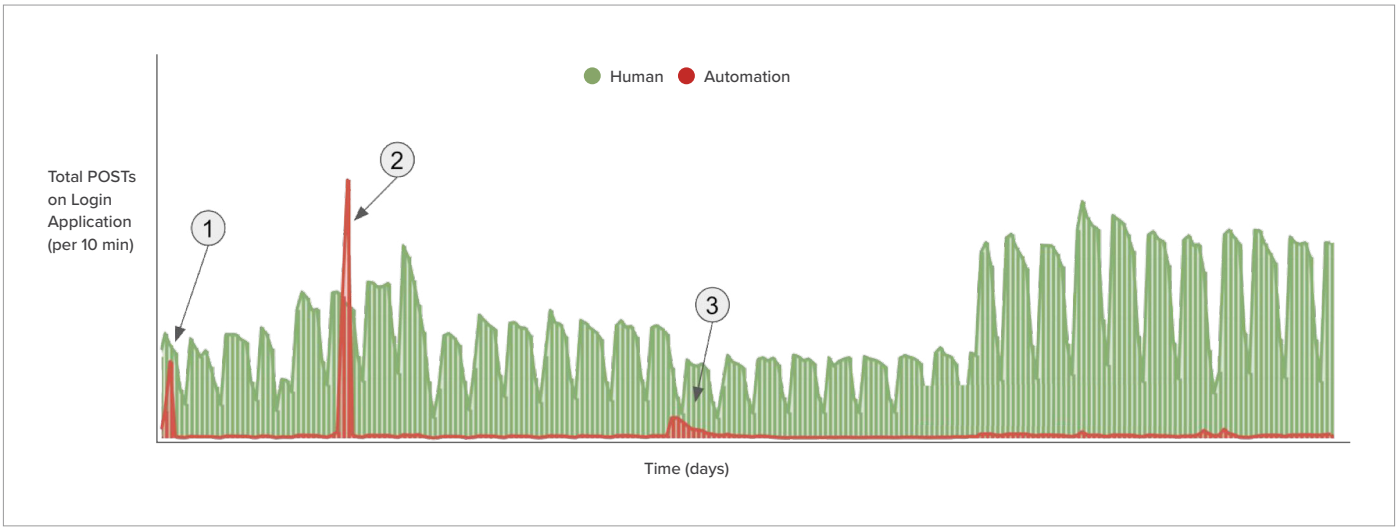


Figure 1: Login traffic during observation mode

Observation Mode

As soon as Distributed Cloud Bot Defense went into observation mode, the provider could immediately see and understand the full nature of its login traffic. As shown in Figure 1, the service distinguished legitimate human traffic (green) from unwanted automation (red) on the login application during observation mode.

Distributed Cloud Bot Defense also delivered advanced threat intelligence reporting to the provider that included insights into the sources of automated traffic. For example, the service identified that half of the automated activity was benign, of which the provider had not previously been aware.

Additionally, during observation mode, Distributed Cloud Bot Defense identified three separate automated campaigns[1], which are labeled 1, 2 and 3 in the chart. These groups represented nearly one half of the automated transactions during the entire observation period. If an attack group tries to bypass Distributed Cloud Bot Defense by retooling, e.g., utilizing new proxies through which to route its traffic or mimicking a different type of browser, the service is still able to identify the attack group based on other signals.

THE PROVIDER ESTIMATED THAT WITH F5 PROTECTING ITS CONSUMER LOGIN AND ACCOUNT CREATION APPLICATIONS, IT WAS ABLE TO SAVE AT LEAST $3.5M PER YEAR IN FRAUD LOSSES.

F5 also looked at each campaign under a microscope. Figure 2 is a focused view of campaign #2 made available to the provider. This campaign was a highly distributed credential stuffing attack launched from more than 25,000 IP addresses. The attacks made up over 50% of all traffic during the three-day-long campaign. The campaign was also notable in that the attacker attempted to navigate a workflow beyond the login flow.

Mitigation Mode

After a nearly six-month observation period, the provider transitioned Distributed Cloud Bot Defense into mitigation mode. The service immediately blocked credential stuffing attacks, preventing thousands of account takeovers. The provider estimated that with F5 protecting its consumer login and account creation applications, it was able to save at least $3.5M per year in fraud losses.

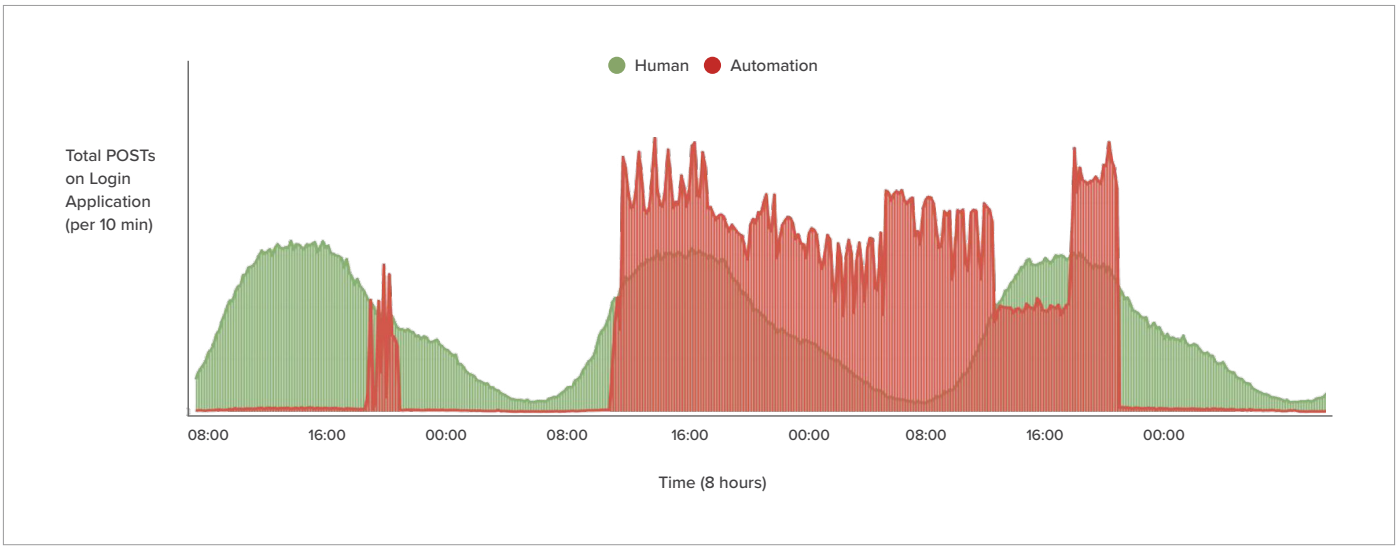


Figure 2: Login traffic during campaign #2

Future Plans

Because of the success of Distributed Cloud Bot Defense in protecting consumer logins on its website and mobile app, the provider is expanding deployment to protect new account registrations for business customers as well as other business applications, including business login, shipping, payment and tracking services.

The provider is also working with F5 to efficiently allow legitimate (benign) automation from business customers who are using automation on the consumer login application to efficiently ship their products.

To learn more, contact your F5 representative, or visit f5.com.

[1] F5 defines a campaign to be a group of automated requests stemming from the same source, as identified by hundreds of proprietary signals.