CASE STUDY

Airline Stops Automated Attacks on Web and Mobile

The Customer: Top 10 Airline—A Top 10 global airline that earns over $15 billion in annual revenue and serves 20 million loyalty program members.

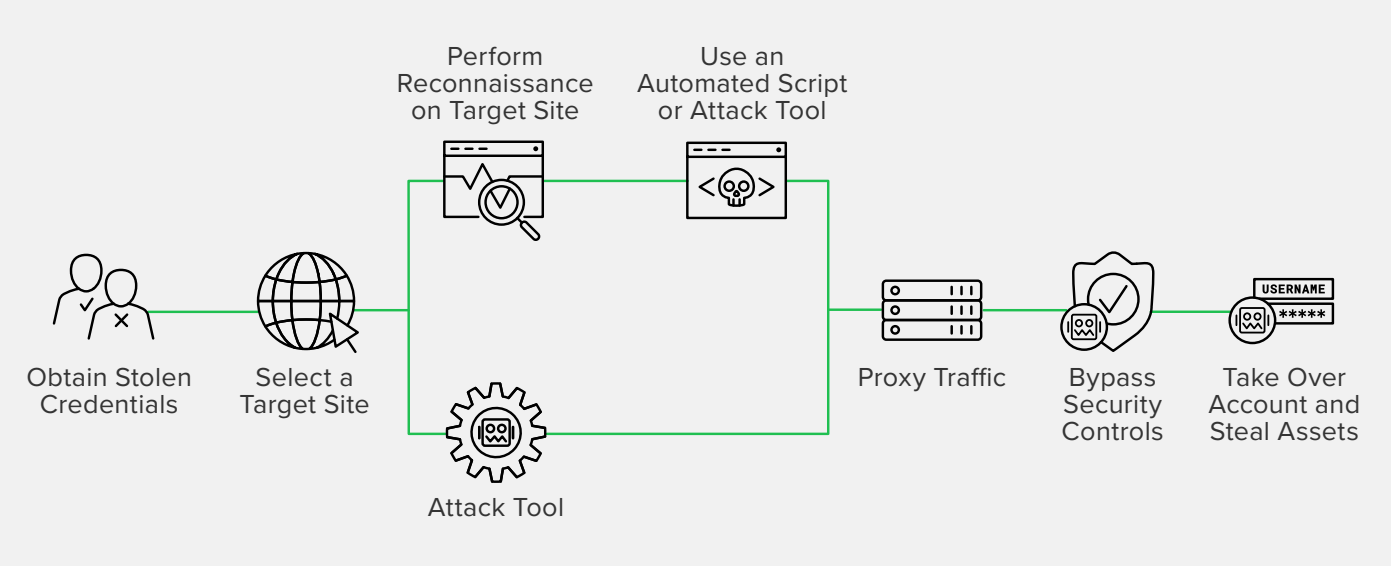

Figure 1: Credential stuffing killchain

Challenge 1: Credential Stuffing

The airline was facing two major types of attacks on its web and mobile applications. First, attackers were performing credential stuffing attacks, in some cases compromising nearly 1,000 customer accounts in a single day.

Credential stuffing is an attack in which bad actors test credentials that have been stolen from third parties en masse on a different login application. Because users reuse passwords across online services, 0.5%–2% of a stolen credential list will typically be valid on a target site, allowing the attacker to take over user accounts.

When attackers successfully took over a customer's frequent flyer account via credential stuffing, the airline's costs included the reimbursement of stolen frequent flyer points 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 to the airline. When an attacker attempted too many failed logins for a certain customer's account, legitimate customers would inadvertently be locked out of their own accounts, forcing them to contact customer service. This consequence of credential stuffing attacks created a customer service burden as well as customer dissatisfaction, which was unacceptable to the airline.

WHY F5?

The airline selected F5 Distributed Cloud Bot Defense for three key reasons:

1. Omnichannel protection including web, mobile, and API solutions
2. Long-term efficacy against sophisticated attackers
3. Holistic platform allowing fraud and security teams to share data

Challenge 2: Fare Scraping

The airline was also facing a scraping challenge. Third parties, including online travel agencies (OTAs) and competitors, ran scripts to gather real-time fare data from applications like "find flights" and "book now." These continual requests exceeded the infrastructure team's capacity to serve customers and also slowed down the site for legitimate customers, causing user friction.

While the airline had partnerships with some of the OTAs, some were acting in poor faith and violating the terms of their data agreements. However, because the airline could not distinguish between legitimate users and unwanted third parties, they were unable to alleviate the problem.

The Decision

When account lockouts peaked in June of 2017, the airline knew it needed to find a solution to credential stuffing attacks immediately. Because F5 was the only vendor that could comprehensively stop credential stuffing and fare scraping attacks while also helping the security and fraud teams prove ROI, the choice was clear. Due to the urgency of credential stuffing, the airline chose to deploy F5® Distributed Cloud Bot Defense first on its web login applications.

Initial Results: Payback in 49 Days

There are two stages to the deployment of Distributed Cloud Bot Defense: observation mode and mitigation mode. In observation mode, F5 analyzes all incoming requests to the application in order to customize its defense and ensure the best possible outcome for the customer. Once F5 and the customer are confident that no legitimate human traffic will be impacted, F5 activates mitigation mode.

During observation mode on the airline, credential stuffing attacks represented over 90% of all login traffic, as indicated by the yellow traffic in the chart below. After four weeks of observation, the airline gave F5 the go-ahead to activate mitigation mode. POSTs from attackers were immediately prevented from reaching the origin server, thereby preventing attackers from successfully logging in.

Attackers will always take the path of least resistance to optimize their ROI. Thus, the vast majority of credential stuffing attackers will move on to easier targets once a defense becomes too difficult to penetrate. Accordingly, within just a week of Distributed Cloud Bot Defense being in active mitigation mode, the sheer volume of attempts decreased by fivefold, as shown by the drop-off in red traffic below.

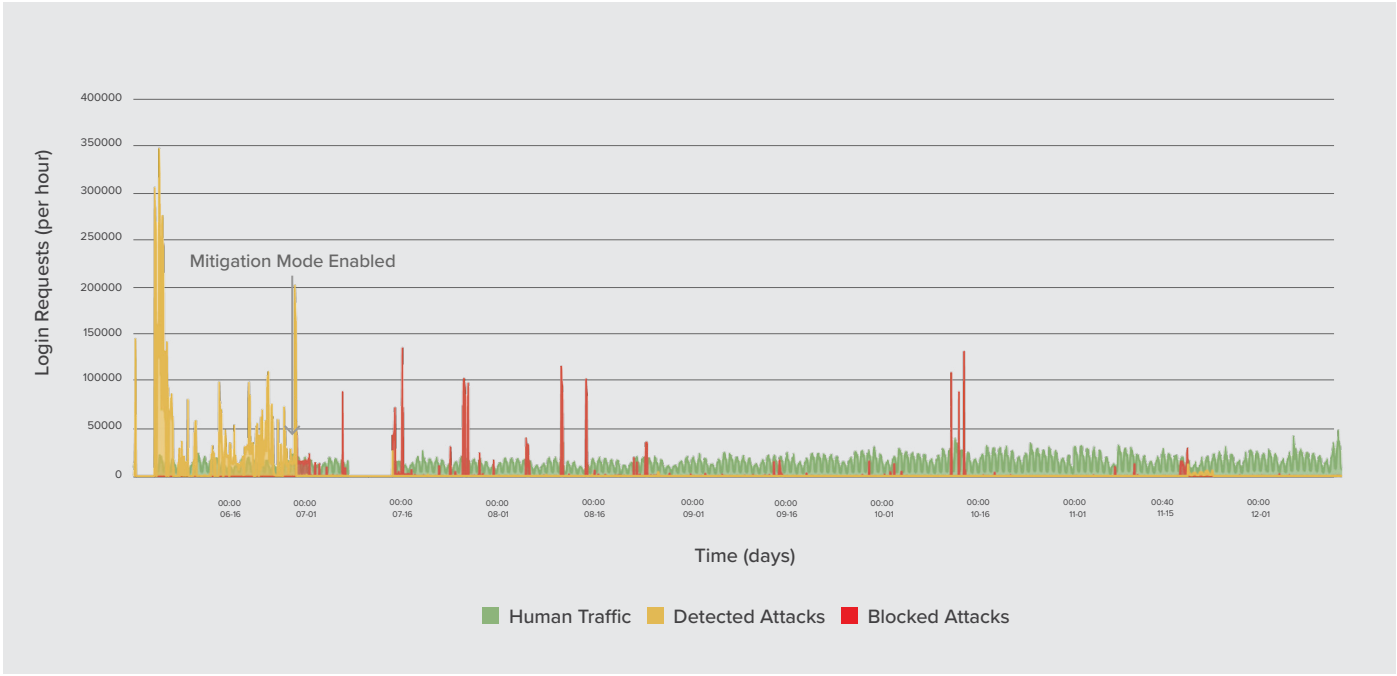

Figure 2: Login requests during the first six months after deploying F5 Distributed Cloud Bot Defense

Long Term Results: Expansion to Mobile

Unfortunately, “easier targets” does not necessarily mean unrelated targets. As more and more attackers became aware that the website was no longer an open door, many turned to the airline’s mobile app.

Because F5 was not protecting the airline’s mobile application and thereby providing visibility into its traffic, the airline did not know the exact distribution of attacks. However, the company had other compelling data that attackers had moved to mobile.

A strong indicator of credential stuffing is the rate at which nonexistent usernames are being attempted on the login application. As depicted in the chart below, the number of nonexistent usernames being tried on web declined steadily after the June deployment, whereas the number of attempts rapidly increased on mobile.

Accordingly, the airline asked F5 to expand protection to its native mobile app, and the SDK solution was fully deployed within a month.

The above chart also shows us that, again, the majority of attackers quickly move on to easier targets once a defense proves too strong. So once it was clear after mobile deployment that neither web nor mobile was a penetrable attack surface, the attackers all but disappeared in December, this time moving on to entirely different targets.

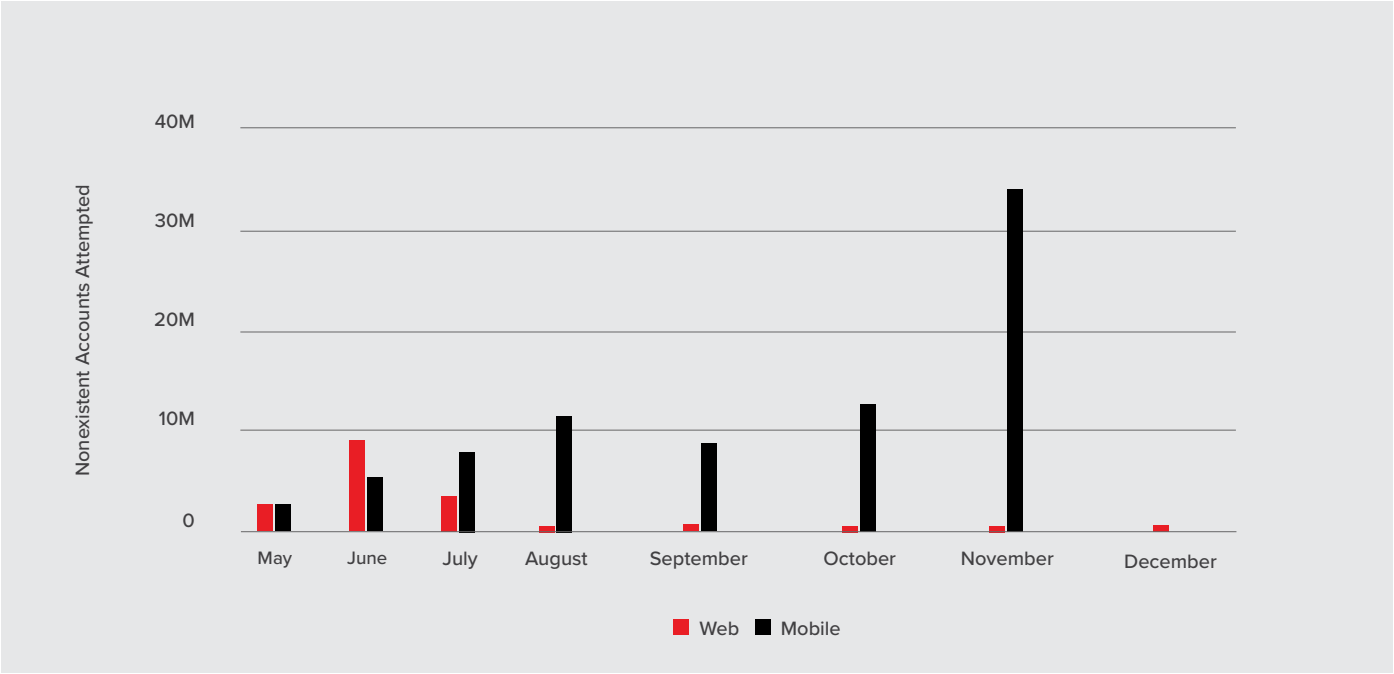

Figure 3: Attackers steadily move to mobile after learning web is defended

WHEN THE CREDENTIAL STUFFING ATTACKS STOPPED, SO DID THE CORRESPONDING FRAUD.

Summary: Holistic & Omnichannel Defense

Most importantly to the airline, when the credential stuffing attacks stopped, so did the corresponding fraud. The security team had known instinctively that attackers were committing fraud after compromising accounts but were unable to link the credential stuffing attacks with account takeover fraud. For the first time, the airline had complete visibility into its traffic via F5's data dashboard, allowing the airline to directly correlate the reduction in malicious login attempts with a reduction in account takeovers and direct fraud losses.

Once F5 demonstrated efficacy protecting the airline's login applications, the airline quickly expanded Distributed Cloud Bot Defense to web and mobile applications being attacked by scrapers. Now that the airline has fully solved automated attacks, the security team has freed up full-time employees to focus on other strategic priorities for the business.

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