CASE STUDY

# Global Dating Platform Defeats Account Takeovers

**The customer—**a global online dating company that serves 35 million members in over 50 countries. The company is a market leader and its mobile app is one of the App Store's top 50 grossing apps.

## The Pain Point

ON AVERAGE 0.5%–2.0% OF A CREDENTIALS LIST WILL BE VALID ON A TARGET SITE.

The company was facing large-scale credential stuffing attacks in 2016. Credential stuffing is an attack in which bad actors take credentials that have been stolen from third parties and test them en masse via automation on the target site. Because users reuse passwords across online services, on average, 0.5%–2% of a credential list will be valid on a target site.

Bad actors were launching sophisticated credential stuffing attacks on both the website and mobile app, leading to numerous account takeovers. Once accounts were successfully taken over, attackers would conduct catfishing and spamming schemes. Not only did these attacks degrade user trust, but they also incurred a substantial cost for the customer service team.

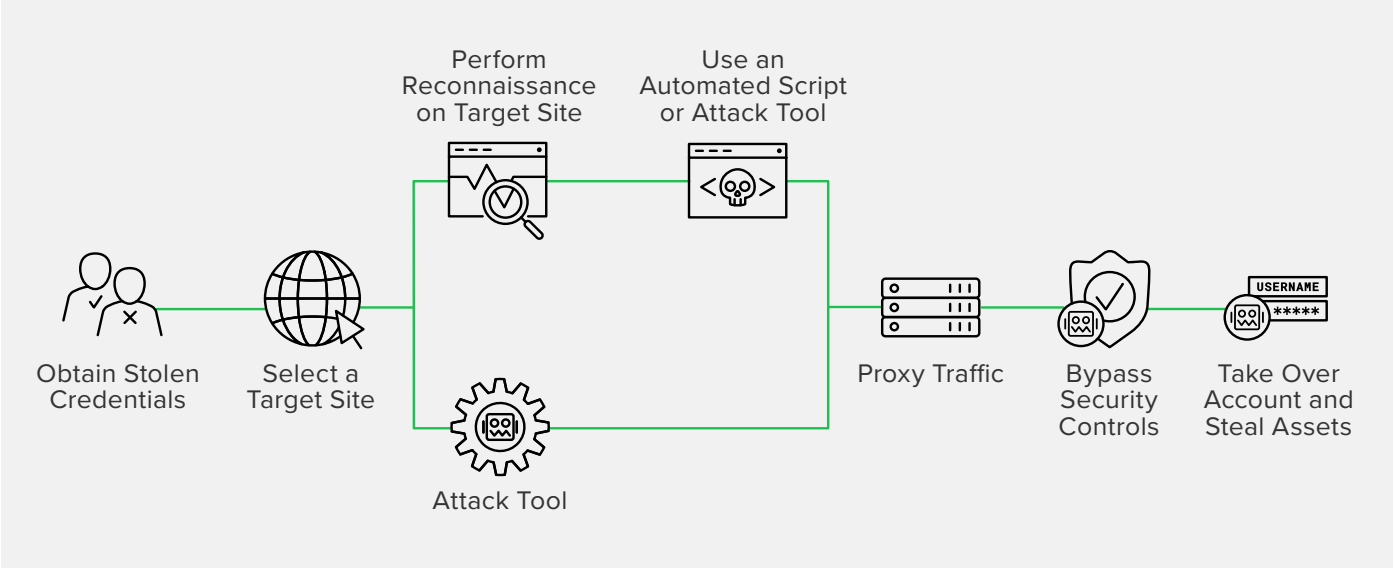


**Figure 1:** Credential stuffing killchain

## The Decision

In 2016, the company evaluated a tool offered by its CDN provider to mitigate the unwanted automation against its web and mobile platforms. After two months of testing the tool, the security and fraud teams were left frustrated. The tool required internal resources to actively deal with every single automated attack, including researching and writing rules for individual activities. The amount of time and resources required to operate the tool was unsustainable

and cost ineffective. Moreover, the tool only identified 20% of the automated credential stuffing activity on the dating website, rendering it inadequate.

When it was clear that the CDN-provided tool was not the right solution, the company contacted F5. It was specifically looking for a solution that could fulfill four critical requirements:

**Figure 2:** Critical solution requirements

| Company Requirement | F5 |
|---|---|
| Protect Against Credential Stuffing | Recognized as the leader in defending enterprises against credential stuffing attacks. |
| Web and Mobile API Protection | Provides both a web and mobile solution. |
| Managed Service | 24x7 service acts as an extension of a customer's security team, so customers do not have to dedicate resources to technology management. |
| Predictable Cost | Service is all inclusive, so sudden increases in attack volume or new system requirements do not incur additional costs for the customer. |

## The Outcome

**As depicted in the traffic chart below, attackers behaved in typical fashion:**
Once the company selected F5® Distributed Cloud Bot Defense, F5 began deployment within weeks. In monitoring mode, Distributed Cloud Bot Defense observed that, on average, 80% of all web traffic was automated. As soon as F5 initiated mitigation mode, the attacks were immediately blocked and prevented from reaching the origin server.

- **Accelerate Days 0-2:** When first blocked, adversaries increase the volume of attack to attempt to break the new defense via brute force.
- **Retool Days 3-7:** After a period of failure, they stop in order to retool their attack.
- **Return Day 8:** The attackers return with a variant of their attack method that they deploy with full force.
- **Give-Up Days 9-10:** The attackers quickly realize that the defense is impenetrable, and they move on to easier targets.

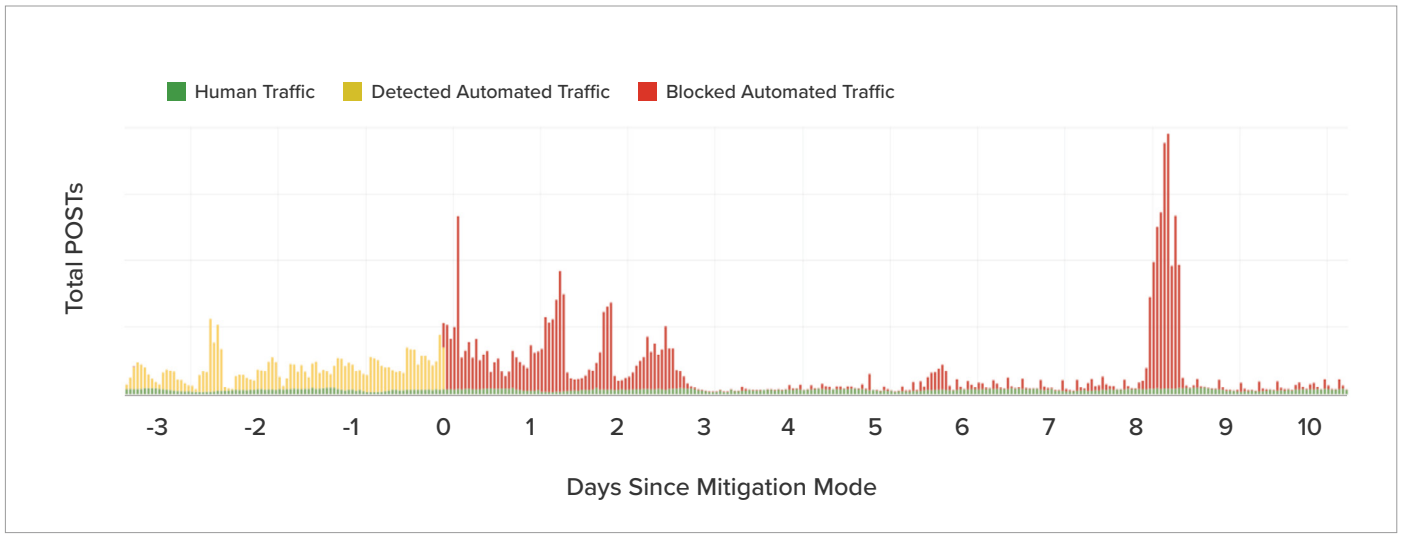


**Figure 3:** Traffic chart

*Note: Because traffic was up to 95% automated during this period, it is difficult to see the layer of real human traffic in green*

By successfully mitigating automated attacks, Distributed Cloud Bot Defense has delivered value across the enterprise:

1. **Security:** F5's managed service has allowed the security team to focus on other security priorities.
2. **Fraud:** Now that Distributed Cloud Bot Defense is preventing a majority of account takeovers (ATOs) from occurring, the fraud team is able to dedicate its resources to detecting and preventing sophisticated manual fraud.
3. **Customer Service:** The reduction in ATOs has led to a decrease in customer service requests and upset users.
4. **IT:** Because automated traffic no longer reaches the origin server, the IT team only needs to handle 20% of the traffic it was were handling before, reducing infrastructure costs. Furthermore, site latency decreased from 250 ms to 100 ms, improving site performance.

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

©2022 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
DC0122 | FUJ-CORP-828820606