CASE STUDY

Top 10 North American Bank Eliminates Credential Stuffing

CREDENTIAL STUFFING

An attack in which bad actors test credentials that have been stolen from third parties en masse on a target login application. Because of password reuse, 0.5%–2% of a stolen credential list will typically be valid on a target site.

The Customer: Big 5 Canadian Bank. A Big 5[1] Canadian bank ("Bank") that earns over $20 billion in annual revenue had been suffering from automated attacks on its web and mobile login applications for months.

Bad actors were performing credential stuffing attacks on all possible channels: both the Canadian and U.S. websites, mobile apps, and even OFX API endpoints. Not only were the attacks leading to account takeover fraud losses, but the sheer volume of attacks also put significant strain on the Bank's infrastructure. The bank was experiencing rolling outages on both their Canadian and U.S. websites, which prevented customers from accessing their accounts. These service outages were unacceptable to the Bank's leadership, so the security team was determined to find a solution.

"A GROUP OF EMPLOYEES ARE SPENDING 100% OF THEIR TIME TUNING OUR CURRENT VENDOR'S SOLUTION, TRYING TO KEEP UP WITH THE ATTACKS. WE NEED SOMEONE TO FIGHT THE ATTACKERS FOR US."

—Director of Cybersecurity

The Challenge: CDN-Provided Tool Insufficient

To mitigate the automated attacks, the Bank first deployed a CDN-provided bot mitigation tool ("vendor"). While the vendor was effective in the short-term, the solution was unable to provide long-term efficacy. The vendor relied on a rule-based system to stop attacks, but the bad actors changed tactics and bypassed those rules within hours, forcing manual configuration of the tool.

The Bank's incident response team was exhausted by the burden of monitoring attackers and configuring new rules 24x7. After months of playing cat-and-mouse with the attackers, the Bank decided to seek out a more sophisticated solution and approached F5.

[1] *"Big 5" refers to the 5 largest banks in Canada and is equivalent to the "Big 4" in other countries.*

The Evaluation: F5 Distributed Cloud Bot Defense vs. Vendor

The security team decided to keep the vendor's solution in place while evaluating F5® Distributed Cloud Bot Defense to compare the efficacy and quality of service of the two solutions side-by-side. For the evaluation, the Bank deployed Distributed Cloud Bot Defense on its Canadian web and mobile login applications.

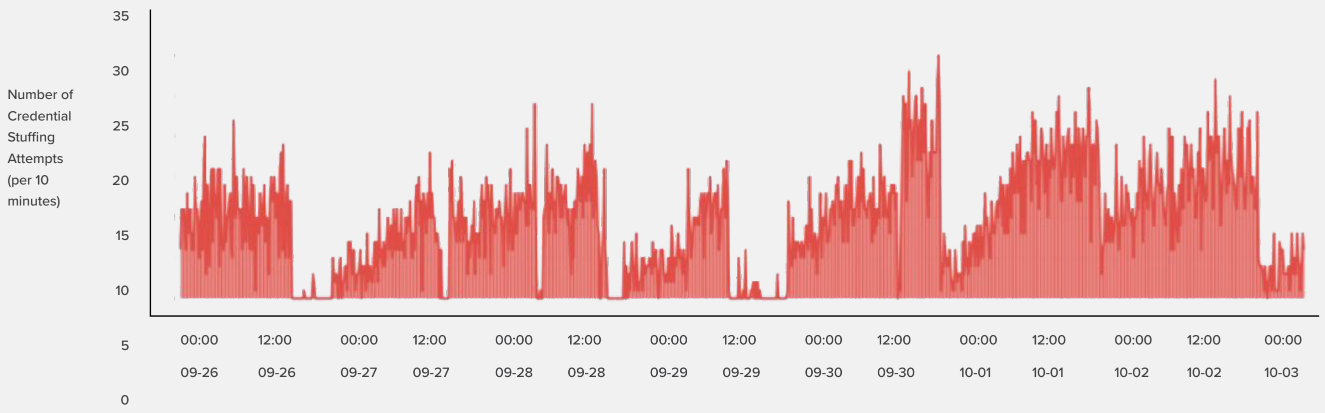
There are two stages to Distributed Cloud Bot Defense deployment: observation mode and mitigation mode. In observation mode, F5 analyzes all incoming requests to the application in order to customize its defense and ensure the best possible outcome for the customer. Once F5 and the customer are confident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

Observation Mode

In observation mode, Distributed Cloud Bot Defense found that nearly 1 out of 10 login attempts were malicious. The Bank was immediately impressed with the service's detection capabilities and the level of insight provided by the Intelligence team during regular briefings.

Distributed Cloud Bot Defense can not only distinguish between malicious and legitimate login traffic, but can also group requests into different attack groups (“campaigns”) for analysis. If an attack group tries to bypass it by retooling, e.g., updating software or leveraging new proxies, the service still correctly identifies the attack groups based on hundreds of other signals.

During the first week of deployment, Distributed Cloud Bot Defense identified four separate campaigns and tracked each of their credential stuffing activity.



9.5k Total posts

2 IPs **1** ASNs **1** UAs

2.32% Success Rate

Figure 1: 220 Successful logins

This is one example of the type of data Distributed Cloud Bot Defense provided the Bank regarding a specific credential stuffing campaign. Insights include the number of IP addresses and ASNs used in a campaign as well as the campaign's success rate, which refers to the percentage of credentials that resulted in a successful login.

Urgency to Activate Mitigation Mode

After five weeks of observation mode, the Bank suddenly became victim to an enormous, unprecedented credential stuffing campaign—the traffic volume grew to a five-time increase from any other prior attack. The Bank was extremely worried because any additional increase in traffic volume would exceed its infrastructure capabilities, which would result in the entire Canadian website going down.

After receiving inadequate help from their existing vendor, the CISO of the Bank personally called F5 with a request: transition from Observation Mode to Mitigation Mode weeks ahead of schedule to stop the debilitating attack. The F5 Professional Services team went to work—within a few hours, Distributed Cloud Bot Defense was configured and deployed in mitigation mode on the Bank's Canadian sites.

As soon as Distributed Cloud Bot Defense went into mitigation mode, as depicted by the transition from yellow to red traffic in the chart above, the attack tempered down. The service completely eliminated the flood of automated traffic from reaching the Bank's origin server, allowing the Bank's incident response team to stabilize traffic and ensure service availability for customers.

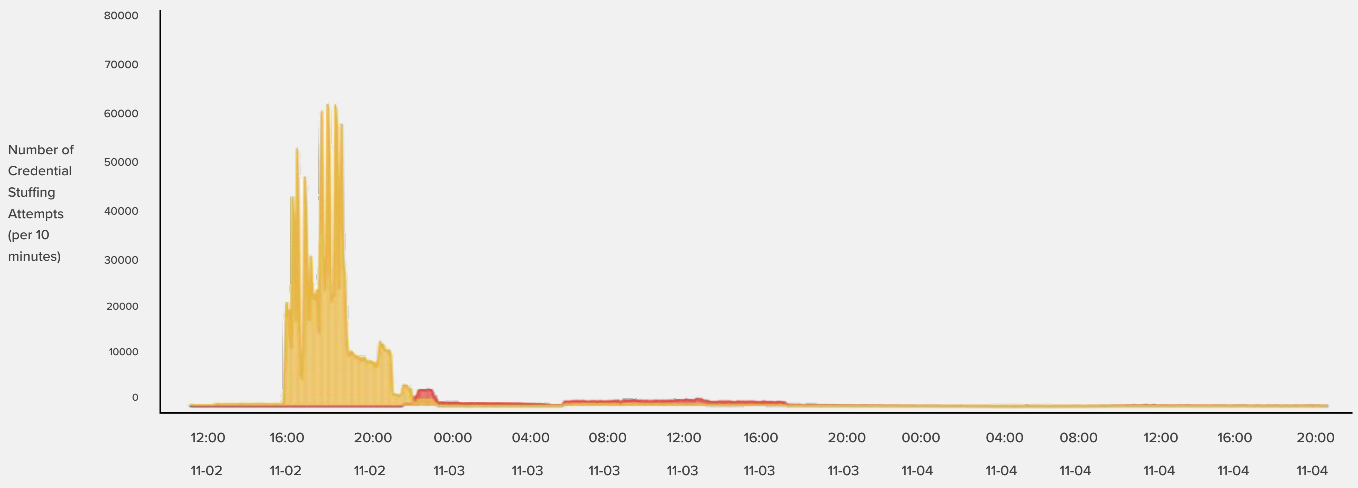


Figure 2 : Distributed Cloud Bot Defense defeated the unprecedented attack immediately

HOW THE BANK IS BENEFITING FROM DISTRIBUTED CLOUD BOT DEFENSE

1. Eliminated malicious login traffic, ensuring site availability
2. Acquired fine-grained control over financial aggregators such as Plaid, Mint and Yodlee
3. Protecting customer accounts from fraud

Future Plans: Full Replacement of Vendor’s Solution

F5—through its Distributed Cloud Bot Defense service and Threat Intelligence team—proved superior to the vendor and successfully pinch-hit in a difficult situation. The Bank appreciated not just Distributed Cloud Bot Defense's efficacy, but also that F5's team was willing and able to deploy in the midst of a large-scale attack.

As a result of Distributed Cloud Bot Defense successfully defending the Canadian login applications, the Bank plans on taking considerable steps into broadening their use of it, including:

- Removing the original bot-mitigation vendor from all web properties
- Expanding Distributed Cloud Bot Defense's coverage to 100% of web and mobile properties across all geographies
- Augmenting fraud analytics abilities by leveraging data available in the service's dashboard

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