SHAPE
Part of F5

CASE STUDY

F5 Enables State Government Agencies to Fight Fraudulent Unemployment Claims

Executive Summary

How one F5 customer took on the growing unemployment fraud problem

During the COVID-19 pandemic, opportunistic hackers saw their chances to exploit the rapidly growing problem of unemployment fraud. Estimates for COVID-19 related unemployment fraud losses were as high as $36 billion in 2020, and every state was impacted in some manner.

The tactics hackers have used during this crisis are as varied as they are dangerous:

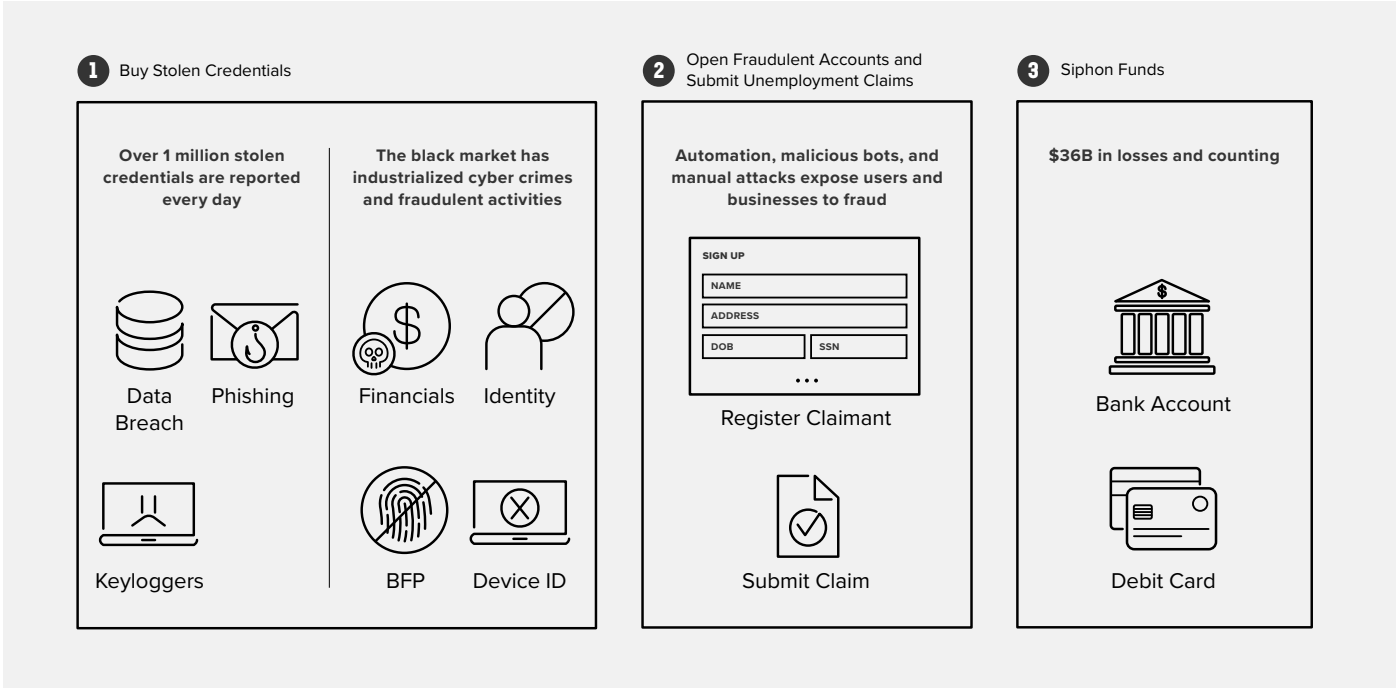

Figure 1: Tactics used by fraudsters

1. Buy stolen identities from the underground via the dark web
2. Fill out unemployment claims *online* using that information
3. Receive unemployment benefits to a drop account or direct payment to a debit card

One of F5's customers faced this challenge head-on. Here's how they used F5's solutions to proactively combat fraudulent unemployment claims.

The Challenge: Combatting Fake Unemployment Account Registrations

Bombarded with unemployment claims at the outset of the pandemic, the agency was under pressure to pay claims first and ask questions later—a welcoming environment for fraudsters.

But, as news of widespread unemployment fraud across the country began to spread, the agency turned to F5 to see if it too had been attacked. F5 made the alarming discovery of several anomalies pointing to an undeniable truth: new accounts were being created by hackers to siphon off unemployment benefits from the agency.

The Solution: Discovering Anomalies with F5 Fraud Prevention

The anomalies F5 discovered, based on the telemetry we collected and analyzed, included:

Copying and pasting activity: Fraudsters were observed copying and pasting data into form fields (e.g., first name and last name). Legitimate users do not normally exhibit this behavior.

Screen toggling: Fraudsters were observed toggling between browser windows, allowing them to cut and paste from a list of stolen credentials.

Odd screen real estate usage: The fraudsters' browser windows left a lot of screen real estate available to accommodate lists of stolen credentials.

Device affinity: On multiple occasions, large numbers of unemployment claims were submitted from the same device.

Environment spoofing: Fraudsters were observed trying to hide and disguise their environment (e.g., browser user agent, OS version, application versions, etc.). F5's anti-spoof technology is one of the best in detecting fraudsters trying to lie about themselves.

Odd time zones: Time zones from around the world were observed—far from the expected behavior for a state with only one time zone.

VPN and cloud-hosting usage: In many cases, the time zone of the device did not match the time zone of the IP address, indicating VPN or cloud-hosting usage—yet another attempt by fraudsters to hide and disguise themselves.

The Result: Stopping Fraud and Saving Tens of Millions of Dollars

The insights observed above, when combined with F5's industry-leading data and world-class AI/machine learning models, provided the agency with an extremely high fraud detection rate and very low false positive rate, helping the organization save tens of millions of dollars.

In short, the agency discovered what nearly every other F5 anti-fraud customer finds: the investment in F5's anti-fraud solution yields a significant multiple of that investment in fraud savings.

To learn more about how we can help you detect and prevent fraud, contact your Shape Security or F5 representative, or visit shapesecurity.com or f5.com.