Global Money Transfer Service Foils Fraudsters, Avoids Outages
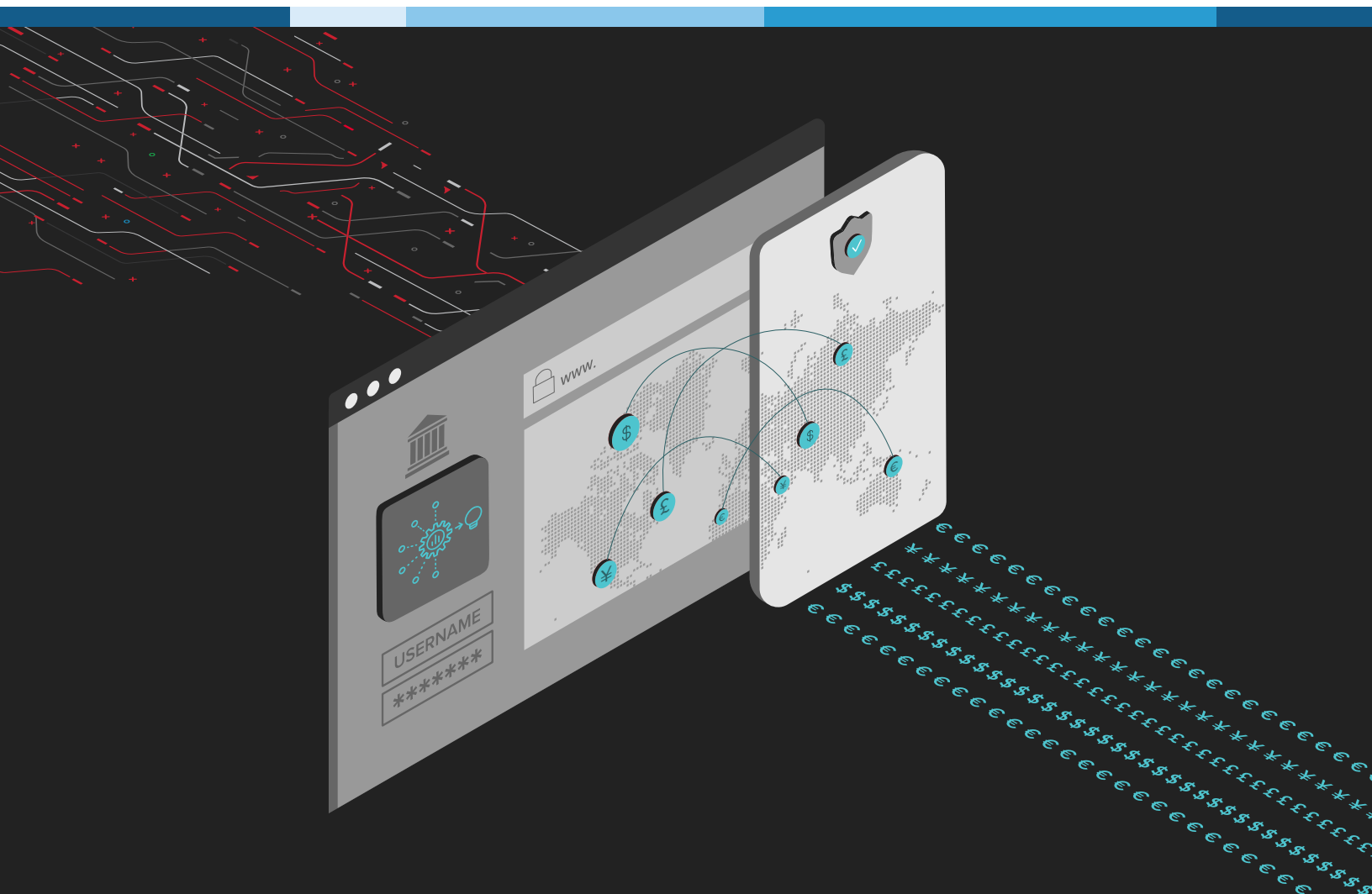
The Customer: Global Money Transfer Service. A top 3 money transfer service, with more than $5 billion in annual revenue, serves customers in over 100 countries. It has hundreds of thousands of agents, millions of clients, and over $200 billion in principal per year. The company recently faced a bevy of challenges that neither it, nor its existing vendors, were able to resolve.
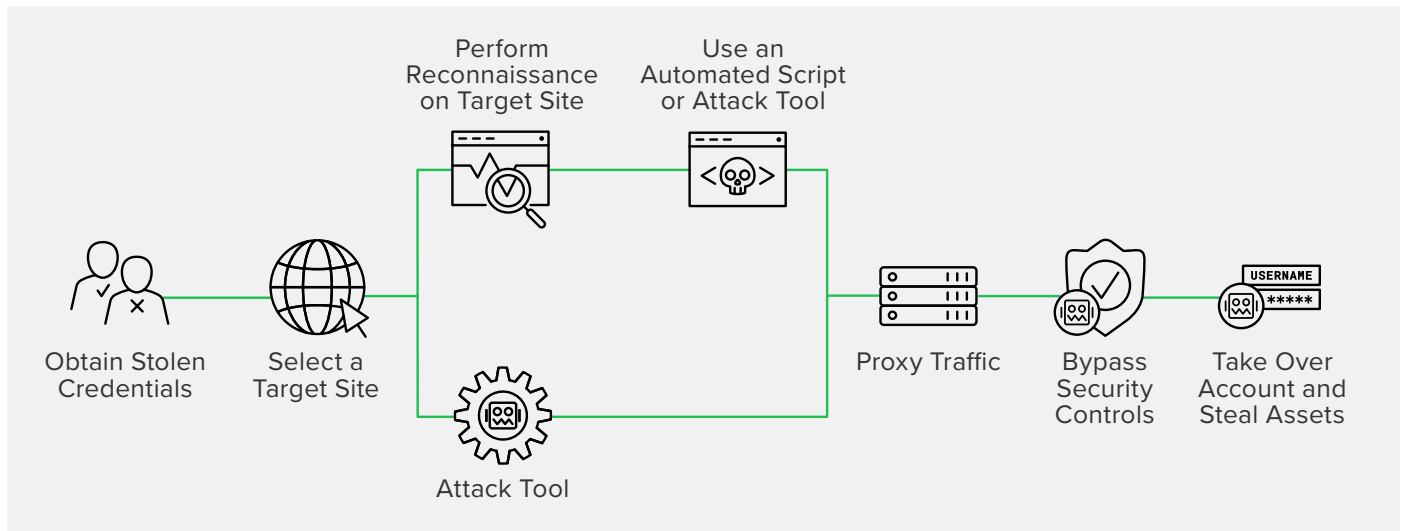

Figure 1: Credential stuffing killchain

Challenge 1: Credential Stuffing to Account Takeovers

The money transfer service was suffering from waves of credential stuffing after each publicized credential spill. 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.

Attackers were using the campaigns of credential stuffing to validate their credential lists, steal money, intercept money transfers, and take over accounts at the money transfer service.

The malicious actors were automating against four key services: the login page, the transaction search, password resets, and email verification.

The validated credential lists were sold to a different set of attackers who would monetize each account takeover by sending themselves money transfers from the associated bank accounts of frequent money transfer users. The attackers were also launching searches looking for transfers-in-transit to recipients, which they would then intercept.

The money transfer service selected F5 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: Server Load Tipovers

If the stolen transfers weren't bad enough, the transaction inquiries launched by the automation were impacting the search database and causing timeouts and outages. The transfer service operates globally, and customers often remit money from rich countries with faster Internet to emerging countries, where "Mom & Pop" corner store agents using Pentium II computers, IE7 and dial-up Internet are common. The transfers were already shaky before the database timeouts; with them, the proper payments could be delayed by days.

Challenge 3: Account Lockouts

The money transfer service's password reset page was besieged with automation, and resets were locking thousands of legitimate customers out of their accounts. Even when no actual fraud against the target user took place, costs were incurred by the service to help the customer regain access to (and secure) their account.

The Decision

The money transfer service had been trying to fight these fires with its CDN and its bolt-on bot management feature to no avail. Whenever the company thought it had an adequate defense in place, the attackers would retool and it would start all over again. Changes were difficult to deploy as the service had hundred of entry points, globally. So the money transfer service called F5.
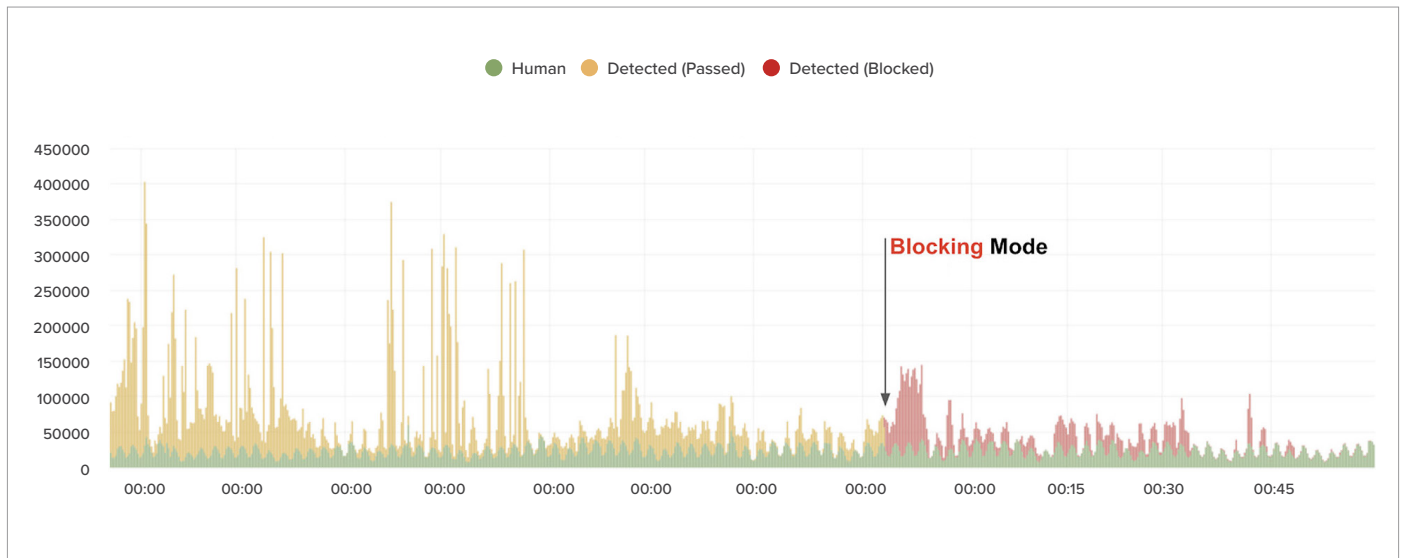

Figure 2: Attack traffic

Initial Results: $786K Saved in First Month

There are two stages to F5® 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.

During observation mode with the money transfer service, Distributed Cloud Bot Defense observed 45 million POST transactions and found that credential stuffing attacks represented over 61% of all traffic, as indicated by the yellow traffic in the above chart. After a quarter of observation, the service gave F5 the go-ahead to activate mitigation mode. POSTs from attackers were immediately prevented from reaching the origin server, preventing attackers from successfully testing credentials or logging in.

Attackers will always take the path of least resistance to optimize their ROI. The majority of credential stuffing attackers will move on to easier targets once a defense becomes too difficult to penetrate. During the first two weeks after Distributed Cloud Bot Defense was put in active mitigation mode, the attackers attempted three different retool campaigns, as shown by red traffic above, before giving up and moving on to easier targets.

Long-Term Results: Expansion to Mobile

Unfortunately, "easier targets" does not necessarily mean unrelated targets. As more attackers became aware that the website was no longer an open door, many turned to the service's mobile apps.

Because the money transfer service had grown aggressively through acquisition and operated in hundreds of countries, it had an astonishing number of mobile applications: over 50. F5 warned the service that as automated web traffic was blocked, the attackers would move to mimicking mobile clients.

50 MOBILE APPS
WERE PROTECTED.

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

F5 worked with the service to integrate F5® Distributed Cloud Defense Mobile SDK protection into all 50 of the mobile applications and blocked the attackers there as well. But the attackers weren't done yet.

F5 had secured the web and mobile sites for the money transfer service, stopping the fraud, server tipovers and email verification campaigns. In a move that surprised the service, the email verifiers launched campaigns against third-party partners of the money transfer service. These trusted partners proxy logins from legitimate customers to the service. The attackers began testing their email verification campaigns across the trusted partners.

The money transfer service urged its partners to adopt F5 Distributed Cloud security solutions, and now F5 services are rolling out in front of all the partners today, and the attackers have given up.

Summary: Holistic and Omnichannel Defense

Most importantly to the money transfer service, when the credential stuffing attacks stopped, so did the corresponding fraud and server tipovers. 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 service had complete visibility into its traffic via the Distributed Cloud Bot Defense data dashboard, allowing the service to directly correlate the reduction in malicious login attempts with a reduction in account takeovers and server tipovers.

Today, F5 protects the service's hundreds of entry points, its dozens of mobile applications, and now its partners as well. The service's 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.