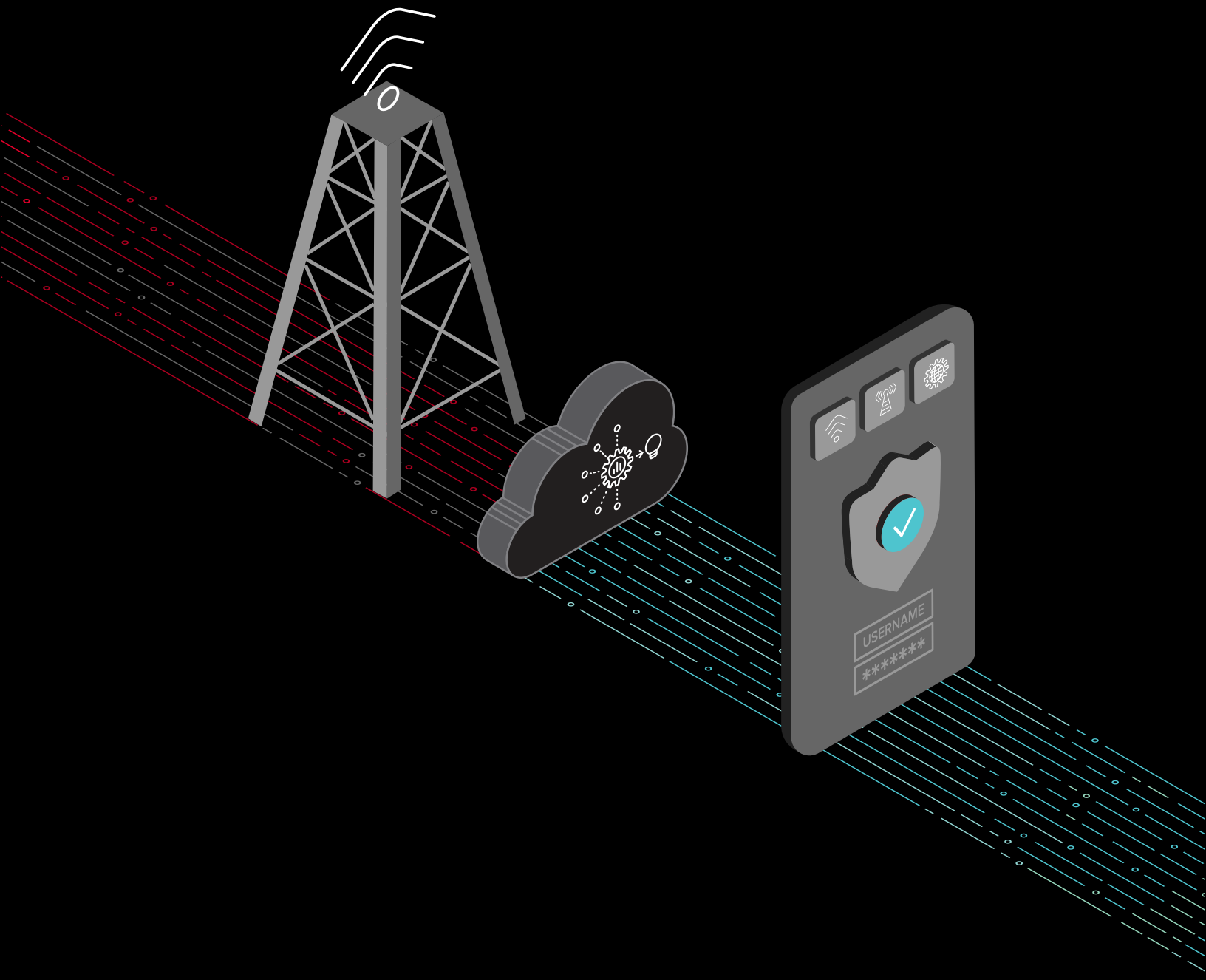
SHAPE
Part of F5

CASE STUDY



Top 3 Telecom Provider Secures Mobile Accounts

The Customer: Top 3 Telecom Provider. A top 3 US telecom provider that earns over $40 Billion in annual revenue and serves nearly 100 million customers.

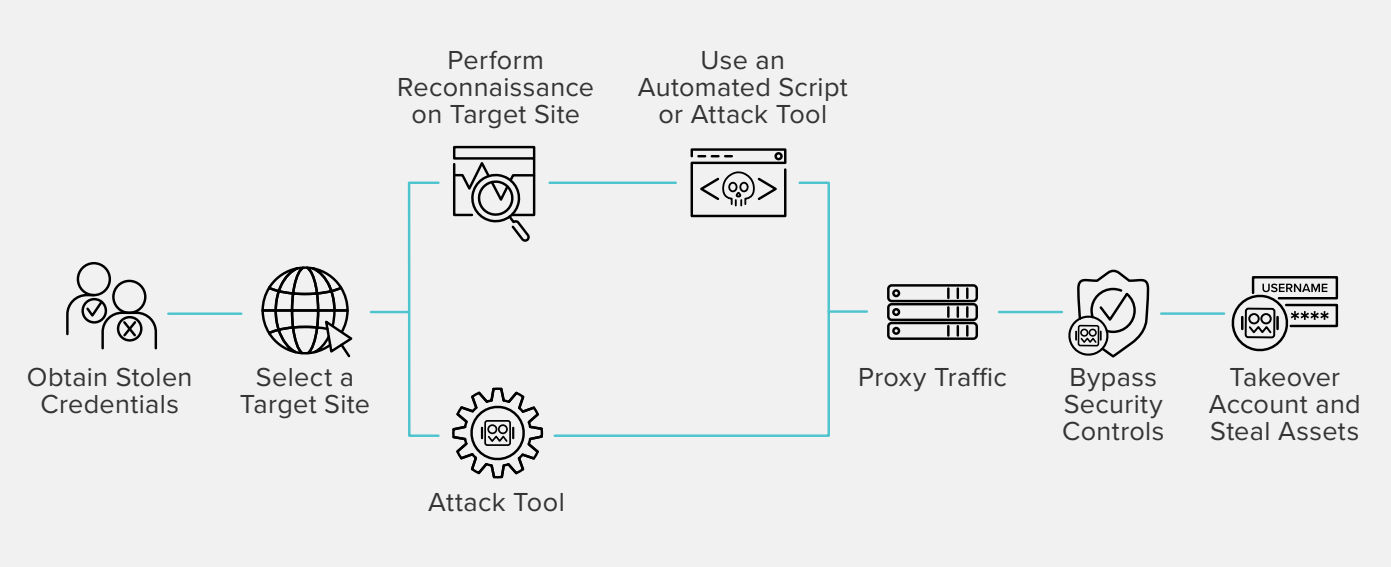


Figure 1: Credential stuffing killchain

0.1-2% OF ALL CREDENTIALS TESTED IN A CREDENTIAL STUFFING ATTACK

Key Challenge: Credential Stuffing

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, 0.1%-2% of a stolen credential list will typically be valid on a target site, allowing the attacker to hijack the user's account.

Attackers typically use automation to conduct credential stuffing at scale. Once attackers validate credentials on a login application, they take over the customer's account to commit fraud.

Over two billion credentials were reported spilled in 2017, so attackers always have fresh credentials to test out on telecom providers. Based on customer data, Shape estimates that the US Telecom industry faces nearly 50 million credential stuffing attempts per day.

Credential stuffing attackers targeted the telecom provider to commit various fraud schemes, including:

Upgrade Theft

After hijacking accounts, attackers take advantage of free and discounted upgrades for which the victim is eligible. Upon ordering the mobile device, the attacker will either direct it towards

a shipping address they control or choose a “pick-up in store” option. If choosing the latter, attackers will have a mule visit the store to pick up the device and then resell on third-party marketplaces such as eBay or Craigslist.

Two-Factor Authentication Bypass

Most consumers that enable 2-factor authentication use their mobile phone as their second authentication mechanism. If an attacker has successfully broken into a customer’s telecom account, then the attacker can circumvent 2-factor authentication that the victim has employed over other accounts including financial and email accounts.

Upon taking over a telecom account, the attacker will call customer service, impersonate the victim, and ask for a new SIM card to be associated with the phone number. The attacker will then be able to intercept any code sent via SMS for 2-factor authentication purposes.

Virtual Calling

Consumers are significantly more likely to answer a phone call originating from their own area code. After taking over accounts, fraudsters would use the telecom provider’s virtual calling feature to place calls to all people that had similar phone numbers, thereby increasing the success rate of their telephone scam.

PAIN POINTS

1. Credential stuffing and the resulting account
2. Takeovers were causing the company many negative consequences including:
    - Subscriber Churn
    - Fraud Loses
    - Call Center Overload

The Decision

When account takeovers became so common that the telecom provider received negative press about the situation, the company knew it needed to find a solution immediately. Because Shape was the only vendor that could comprehensively stop credential stuffing, the choice was clear. Due to the relative urgency of the problem, the telecom provider chose to deploy Shape Enterprise Defense on not only its web login, but also its password recovery and account creation applications.[1]

Results: 94% Automation Detected

During the first week of deployment, Shape detected that 94% of all traffic on the login application, or nearly 65 million posts, was automated. Of that, over 50 million requests were credential stuffing attacks, all of which Shape could prevent from reaching the origin server.

Shape was also able to shed light on to the other types of automated traffic the telecom provider was receiving. For example, Shape identified over 100,000 POSTs that were coming from the financial aggregator Mint.

Financial aggregators like Mint operate as web scrapers. They ask for clients’ real credentials to their financial accounts, login on their behalf continually, scrape financial data, and present

the data in their own app. Mint, in particular, provides an automated bill-paying function which some of the telecom provider's customers use, hence the steady POSTs. The telecom provider was pleased that Shape had identified this previously unknown source of traffic, as they could now observe and manage aggregator traffic.

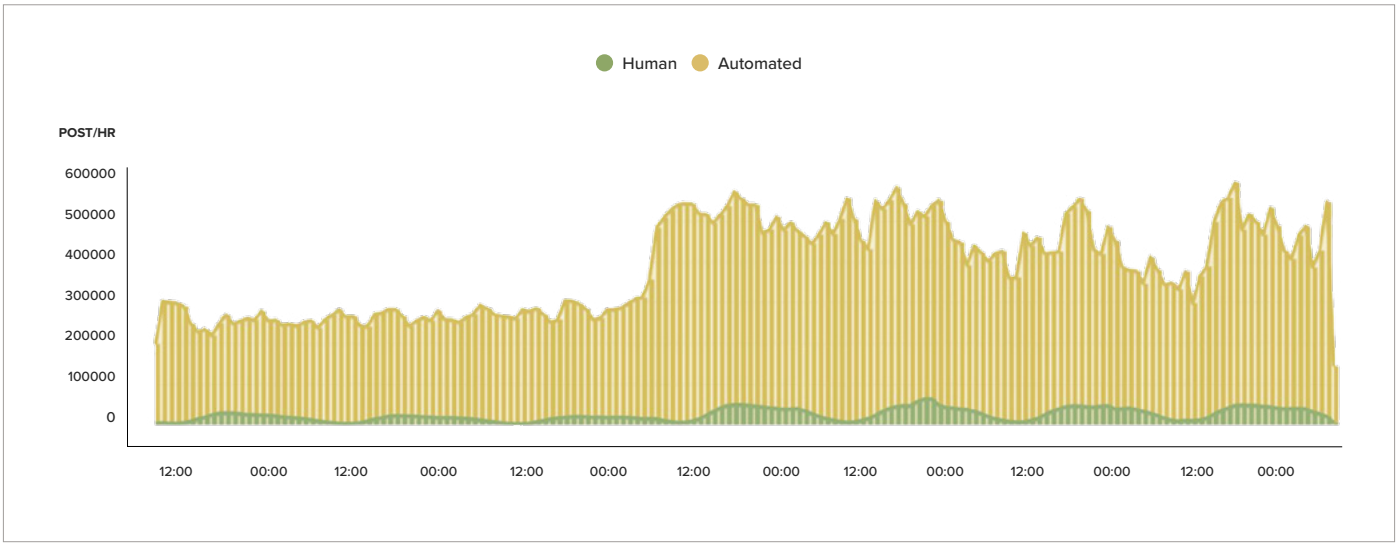


Figure 2: Login traffic during the first week of deployment

Next Steps: Mobile Protection

Attackers will always take the path of least resistance in order to optimize their ROI. Thus, the vast majority of credential stuffing attackers move on to easier targets once a defense becomes too difficult to penetrate. Many of Shape's customers observe that, within the first weeks or months of Shape Enterprise Defense actively mitigating attacks on web applications, the attackers move over to targeting their mobile app.

The telecom provider is an extremely attractive target to attackers, as demonstrated by the large volume of credential stuffing traffic. A portion of these attackers are guaranteed to move on to the mobile app (as opposed to just move on to another company completely), so the telecom provider will soon expand protection to its mobile app.

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

[1] These two applications are often used by attackers to improve credential stuffing and account takeover success rates.