CASE STUDY

International Airline Fights Fare Scrapers

Overview

Data stolen by scrapers—A major international airline has 30 websites, offered in 11 languages, to provide flight information and host frequent flyer accounts. Cybercriminals and fare aggregators have compromised customer accounts and misappropriated airline information using automated attacks.

In 2014, cybercriminals compromised a large number of frequent flyer accounts using an automated credential stuffing attack. The subsequent theft of frequent flyer miles attracted international press attention, drew negative social media commentary, and created customer dissatisfaction.

Aggregators used scraping bots to discover and publicize non-compliant ticketing options. These unauthorized bookings disrupted the airline's ability to manage revenue and reduced the airline's operational flexibility.

These attacks were economically motivated. Travel aggregators monetized airline information by charging commissions or selling advertisements. Cybercriminals resold stolen award tickets or frequent flyer miles on Darknet markets.

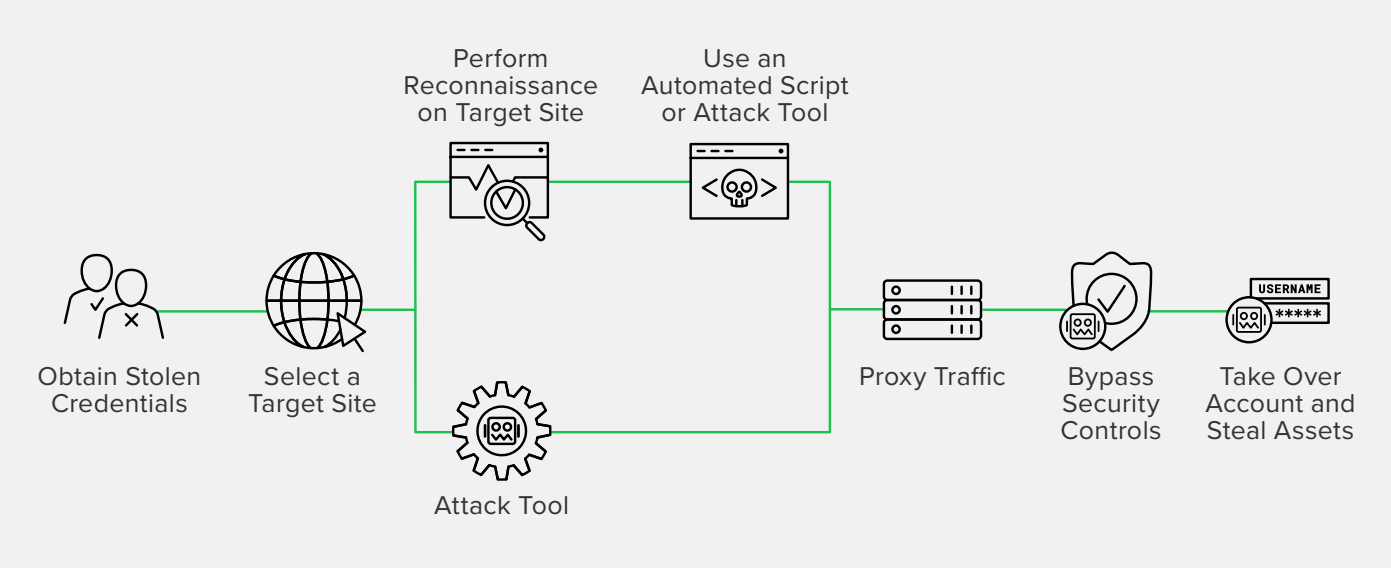


Figure 1: Credential stuffing killchain

Attack Target

Scraping bots targeted the airline's search function to extract route information that was repackaged and offered to the aggregator's customers. Automation accounted for about a quarter of search traffic on the airline's main search URL. Over a very short period of time, scrapers executed more than 850,000 automated searches.

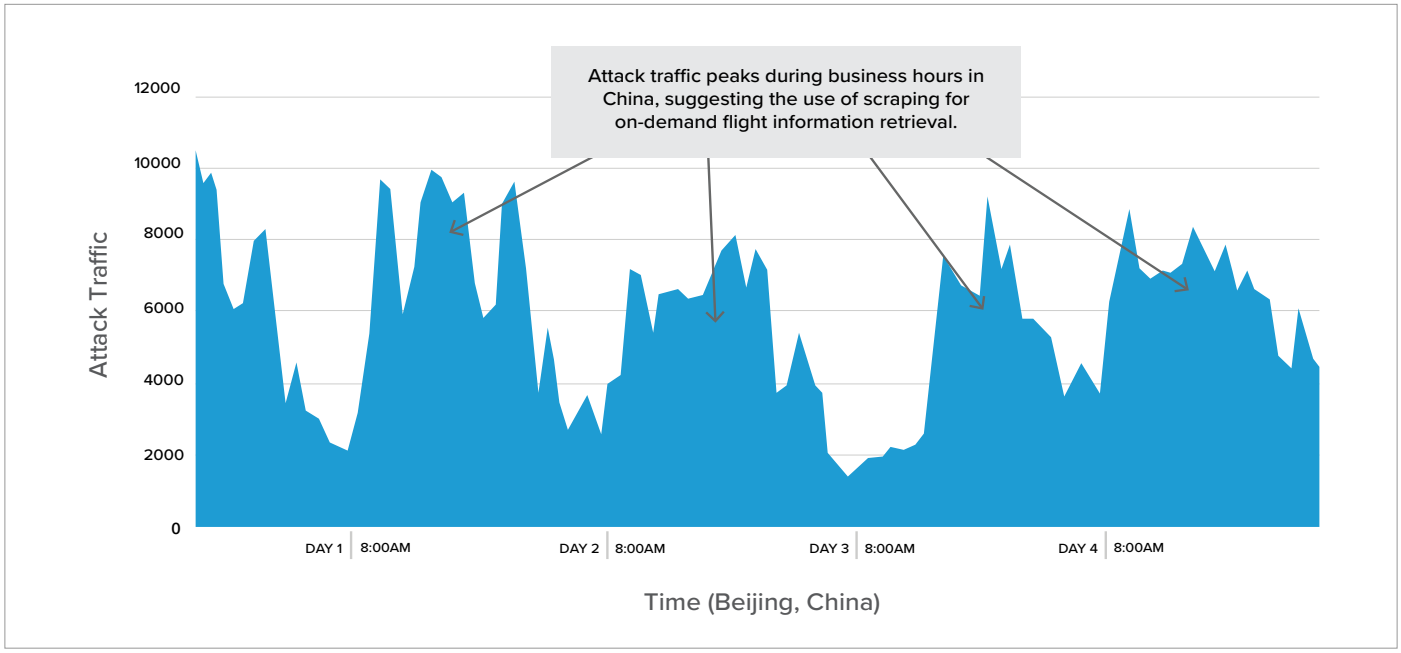
Attack Methods

An unusually large botnet, using many different IP addresses, was engaged to execute scraping attacks on the airline. About 85% of the unwanted traffic came from China. The majority of these scrapers used simple HTTP-only tools. F5 also observed the use of a credential stuffing script. This script, and other tools like it, use automation to test usernames and passwords stolen from other sites.

Attack Impact

Multiple distinct bot groups were observed. Traffic rates for the group with the highest transaction volumes peaked during business hours in China, suggesting that this group was providing on-demand flight information to the Chinese market.

The chart below (a representation of data taken from the F5® Distributed Cloud Protection Manager dashboard) illustrates the ebbs and flows of the attack. Note that all traffic on this chart is from the attacks. Legitimate traffic is not shown.



Failure of Existing Security Solutions

The airline protects its websites with layered defenses that include web application firewalls, IP reputation checkers, rate limiters, and other security solutions. Even though each element worked as intended, the attacks evaded existing defenses by closely mimicking legitimate search and login attempts.

To further camouflage their activities, adversaries leveraged proxies and large botnets to make each search or login attempt appear to come from a different visitor. Traditional security solutions, designed to prevent known attacks, blacklist IP addresses, or block excess traffic from a single host, were easily bypassed by these highly evasive methods.

Attack Mitigation

The airline's web platform uses AJAX pages to deliver a responsive and highly available visitor experience.

F5® Distributed Cloud Bot Defense deflected all automated traffic and kept it from reaching the airline's website. Credential stuffing attacks were completely mitigated. Automated fare scraping is allowed to continue for investigation, but can be blocked at any time.

Conclusion

Bots and evasive methods were used for the theft of proprietary flight information and the takeover of customer accounts. Existing website defenses were ineffective against automated adversaries masquerading as human visitors. Distributed Cloud Bot Defense, which deflects even the most sophisticated bots, reliably stopped these website attacks.

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