THE ESSENTIAL GUIDE TO CREDENTIAL STUFFING IN FINANCIAL SERVICES
CREDENTIAL STUFFING IN FINANCIAL SERVICES

If a bank account is accessed using the correct login credentials, how can you identify the legitimacy of the user vs. an automated traffic attack?

In 2018, a new incident of financial fraud was identified every 15 seconds¹. The gravity of the cybercrime challenge is driving financial institutions to invest heavily in tackling the problem, with an estimated £650 million spent annually on dedicated employees to combat fraud and money laundering amongst other financial crimes².

Over the last 12 months, the cyber threat landscape in the financial services industry has shifted, as the accessibility of mass data dumps and proxy servers has created a breeding ground for credential stuffing attacks.

Credential stuffing attacks are exposing financial institutions to varying degrees of fraud and theft, creating an urgent need to take proactive measures that minimise risk to your customers and cost to your business.

WHAT IS CREDENTIAL STUFFING?

Credential stuffing is the practice of using usernames and passwords to fraudulently take over user accounts.

Data dumps consisting of millions of unique combinations of usernames and passwords, are readily available at scale and little to no cost. Although a portion of the data in a given dump is likely to be stale, poor password hygiene and password reuse means that even old data can be valuable to attackers, looking for Personally Identifiable Information (PII) for malicious gain.

With this multitude of PII to hand, automated web injections are used to carry out multiple login attempts at a time against the targeted online accounts in brute force stuffing attacks. Once an attacker has one password for a user, the greater the opportunity to find another account belonging to the same user and exploit this also.

WHAT IS THE THREAT TO FINANCIAL SERVICES?

According to the Financial Conduct Authority (FCA), the UK banking industry lost an estimated £1.2bn to fraud and scams in 2018⁴.

Credential stuffing gives attackers unlimited access to account and transaction details that can be used to apply for a loan, a credit card, carry out bank transfers or exploit your organisation for a bank-breaking profit.
Without the necessary bot management technology in place to identify anomalies in traffic patterns and behaviour, automated traffic threats often go undetected.

“\n
In 2018, 24% of external attacks were carried out using stolen credential logins or encryption keys.\n
\n
CREDENTIAL STUFFING IN ACTION

Throughout 2018, financial institutions have been persistently bombarded with credential stuffing attacks that last for days at a time. The magnitude of such attacks exposes organisations to significant financial and reputational damage as a variety of PII is accessed including names, addresses, transaction history and account numbers.

The enforcement of the General Data Protection Regulation (GDPR) in May 2018 and the introduction of a two-tier fine system, highlighted the need for personal data security on an international scale. In the event of a breach, failure to comply with the regulation can result in fines of up to 4% of an organisation's global annual turnover.

It is vital that your organisation prioritises securing your web facing applications from all attempts to access and exploit your customers’ PII.

PROACTIVE STEPS TO PREVENT CREDENTIAL STUFFING

Netacea use a range of approaches to detect credential stuffing attacks. At a simple level the built-in reputational analysis and blacklists of known bad actors can easily weed out the less sophisticated attempts.

Intent Analytics powered by machine learning detects account takeover attempts by spotting patterns of behaviour, including spotting indications of an upcoming attack, such as large amounts of fake account creations that can be used to camouflage an account takeover attack, as well as attacks themselves.
WHAT DOES PSD2 MEAN FOR SECURITY IN FINANCIAL SERVICES?

The European Union's (EU) Second Payment Services Directive (PSD2) was implemented in 2018 to reduce the bank's monopoly on customer account information and payment services. Banks throughout the EU have until 14th September to comply with the directive, including providing third parties with access to customer accounts via open APIs.

APIs enable third party payment companies to deploy their own solutions for businesses and customers, which can be integrated with data held by the financial service or bank. APIs provide third parties with easy and secure access to the products and services available via PSD2 compliant developer portals.

The need for APIs for PSD2 compliance highlights the potential vulnerability of APIs sat between financial institutions and third parties if they are improperly secured.

At Netacea, we apply our pioneering technology across all the attack vectors, with one single solution covering website, mobile and API traffic without the need for multiple products or complex mobile SDKs. This approach allows financial organisations to gain insight and control over attacks coming from third party applications or partners who use their APIs.

SMARTER BOT MANAGEMENT

Netacea takes a smarter approach to bot management, driven by machine learning to offer incredible speed, accuracy and transparency to solve the complex problem of credential stuffing.

Netacea understands bot behaviour better than anyone else, thanks to a pioneering approach to detection and mitigation. Our Intent Analytics engine focuses on what the bots are doing (not how they're doing it), so malicious bots are hunted out and genuine users are always prioritised.

Powered by machine learning, Netacea's multi-dimensional approach provides an innovative and profoundly more effective alternative to the traditional 'black box' or JavaScript reliant solutions. It provides frictionless access for genuine users in real-time, while preventing non-human traffic from compromising your business. You'll have the actionable intelligence you need, when you need it, so you're empowered to make smarter decisions about your traffic.

Speak to a data scientist today to find out more about credential stuffing mitigation from Netacea, simply complete the form or book a personalised demo.

Netacea provides advanced insight and visibility into your web traffic, allowing you to create powerful actions based on deep machine learning insight, using APIs. Visit Netacea.com to find out more.


³Forrester, State of Application Report 2019 p. 4 - “In 2018, 24% of external attacks were carried out using stolen credential logins or encryption keys”.