approov
API THREAT PROTECTION

CASE STUDY

Blocking Fraudulent Activities to Protect Reputation and Revenue is Critical in Fintech

"Approov API Threat Protection was a natural choice at the end of our research because of the extensive capabilities of the product."

— Fintech CTO

The advent of PSD2 and open banking has brought both opportunities and challenges for bank and financial institutions in delivering mobile access to their customers. Open banking uses Application Programming Interfaces (APIs) to enable third parties to access financial information needed to create new applications and make transactions.

But APIs are also an increasingly attractive attack vector, creating vulnerable points of attack which require new security techniques as they are not adequately protected by traditional network perimeter defenses. Banks and financial institutions especially, need to ensure these channels are protected in order to mitigate revenue loss and reputation harm.

Challenges

Shortly after launching their service, a fast growing European Fintech company that focuses on digital banking and payments discovered that fraudsters were using automated systems to open multiple accounts using their mobile APIs.

Onboarding of new customers is well understood as a weak point in security flows because, by definition, it is necessary to trust the applicant with a limited set of data. It is therefore a process which is naturally subject to many attempts to automate account creation through scripts which impersonate the traffic coming from the mobile app.

Reviewing activities in account creation, they realized that bad actors had automated the sign-on process and were creating tens and even hundreds of false accounts. They further recognized that they could not counter the scripts by only knowing who was accessing their API; they must also know what was accessing it.

As with many companies in the digital banking/payments sector, the priority for this Fintech company was to grow their customer base as fast as possible so that they reach critical mass quickly. To that end, it was vital that they provided accessible financial services to everyone, in an easily adoptable way, without adversely impacting the convenience that customers had come to expect from apps on their mobile devices.

Equivalent to the way they used Google's ReCaptcha services to protect their website channel, the Fintech company wanted to be able to monitor and control access to their backend services from their mobile apps via their APIs so that fraudulent traffic could be blocked while maintaining a frictionless experience for legitimate customers.

How Approov API Threat Protection Helped

Adding Approov API Threat Protection prevented scripts and bots which spoof mobile app traffic from accessing their API since Approov enables blocking of illegitimate API

requests that were not originating from the official app.

In order to combat bad actors in action, it is important to understand their objectives as well as their methods. Creation of large numbers of banking or payment accounts opens the opportunities to launder money through those accounts for highly sophisticated criminal outfits. On a lower level these accounts can be used to redeem special offers on a grand scale, such as discounts or free periods on music/video subscriptions which might be offered on a per new account basis. There is a vibrant secondary market for such discounted or free services.

By integrating Approov into their mobile channel, this Fintech company achieved a significant drop in fraudulent traffic and eliminated the automated onboarding of new fake accounts.

The Fintech CTO explained why Approov was the right choice:

> ***"Approov was a natural choice at the end of our research because of the extensive capabilities of the product. It required minimal integration work while providing maximum security and flexibility. The similar solutions we found were too rigid and required too much initial integration work."***

Having regained control of the account creation process, it was always going to be important to be vigilant as fraudsters are inventive and may find different ways to combat and circumvent security mechanisms.

One such recent example was the use of Cloner Apps by end users in order to have multiple instances of the same app running on a single mobile device. This in and of itself may not be a problem but, as we covered in one of our blog posts, the installation and use of Cloner Apps open some pretty serious security holes, and the use of Cloner Apps should be banned in most cases.

A capability was quickly added to Approov to detect the presence of Cloner Apps, and it was downloaded to all existing Approov-protected apps via an over the air update. Thus, all customers could - without requiring an app update - immediately see if their customers were using Cloner Apps. If so, and if the customer decided to ban the use of such apps, the security policy could be updated over the air, and blocking could be implemented immediately. Fraudsters usually expect new security capabilities to require a new app release, so they will use the old version for as long as possible, often resulting in a significant delay before a new capability can be enforced. Not with Approov.

The Fintech CTO neatly sums up his feelings on Approov:

> ***"We are very happy with Approov. It works well and matches exactly to the use cases we were initially concerned about. We have also found the Approov team to be very flexible and proactive with respect to managing our service. They are very vigilant, for example around the Cloner App issue, and responsive to any requests we might have."***

To see Approov API Threat Protection in action and get more information, contact us for a free demo.

www.approov.io