approov
API THREAT PROTECTION

CASE STUDY

papara

How Papara Reduced Costs Due To Fraudsters By 90% In 30 Days

"Having completed the integration and test in less than 30 days, we deployed the Approov protection and instantly saw the costs due to the fraudsters drop by 90%."

– Emre Kenci, CTO, Papara

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

However APIs are an increasingly juicy 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 in particular need to ensure these channels are protected in order to mitigate operating costs, revenue losses and brand reputation harm.

The Client

Papara is a fintech that prides itself on offering innovative financial solutions which put the user first and are highly differentiated from products offered by traditional banks. The company was formed in 2015 and launched its first product 1 year later.

As the first non-bank to issue a MasterCard logo prepaid card in Turkey, Papara hit the ground running upon launch and is now a MasterCard, Visa and Interbank Card Center member. Millions of users take advantage of Papara's services each day and the company has quickly become a significant player in the Turkish financial services scene.

The Challenge

Shortly after launching their digital banking and payments service, Papara discovered that fraudsters were using automated systems to open multiple accounts using their mobile APIs. These activities directly led to increased processing costs to the company, in addition to impacting revenue growth. The costs generated by the fraudsters threatened to upset the company's financial balance in spite of its phenomenal growth.

To appreciate better what was going on, it is important to understand that Papara offers merchant accounts for businesses and personal accounts for individuals. Payments made to/from merchant accounts incur a processing fee but payments to/from personal accounts are free. Therefore, some businesses - or people offering a service to businesses - were automating the process of setting up personal accounts which are then used to receive payments from individuals. Using this approach the transfers become peer to peer money transactions so in addition to reducing Papara's income as previously noted, they also negate the legal protections inherent in

commercial payments.

On a lower level these accounts can also be used to redeem special offers on a grand scale, such as discounts or free periods on subscriptions such as Netflix, Spotify and YouTube which might be offered on a per new account basis. There is a vibrant secondary market for such discounted services which can be offered via virtual cards.

Another use case which contributed to increased business costs was account takeover. Phishing websites are created by fraudsters, promising services and offers to Papara customers. Entering Papara credentials is all that is required to access these special deals but of course the real purpose is to collect valid credentials so accounts can be taken over and used for fraudulent purposes. Any money in the accounts will be taken and the account may then be used to transfer other funds between this account and many other accounts - something that can only be done through automation. The result is that the funds are near impossible to track. Papara works with a company who looks for these sites and shuts them down but sometimes the phishing sites operate unknown for some time, hurting the victims and costing Papara money.

Onboarding of new customers is of course well understood as a weak point in the security flow because, by definition, it is necessary to trust the applicant with only a limited set of data. There is therefore a constant battle against attempts to automate account creation through scripts which impersonate the traffic coming from the mobile app.

Reviewing activities in account creation, Papara realized that bad actors were running scripts to automate the sign-on process and were creating tens and even hundreds of fake accounts. The account takeover use case also relied upon automated scripts. The team concluded that they could not counter the scripts by only knowing who was accessing their API via user authentication; they must establish that their mobile app was also present.

Emre Kenci, Papara's CTO, sets some context:

> ***""It has been a driving principle within Papara that the financial services we offer should be available to everyone, in an easily adoptable form, with the convenience that customers expect from mobile apps. However, as we quickly discovered, this has significant implications for platform security."***

Due to the success of the Papara mobile-first banking platform, both the costs incurred by the fraudsters and the lost revenue they caused were growing fast. The company knew it had to take action in order to dramatically cut the fraudsters' activities and bring the company's costs back under control.

How Approov API Threat Protection Helped

Equivalent to the way they used Google's ReCaptcha services to protect their web channel, Papara wanted to ensure that only their mobile apps could access their backend services. If such a solution could be found, fraudulent automated traffic could be blocked while maintaining a frictionless experience for legitimate customers.

Since Approov API Threat Protection verifies that a genuine and unmodified instance of the mobile app is present when each API request is made, it prevents scripts and bots which spoof mobile app traffic from accessing the Papara API. Approov enables the blocking of illegitimate API requests that did not originate from the official app.

Emre explained why Papara picked Approov:

> ***"Approov was a natural choice at the end of our research because its capabilities met precisely the need we had. 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."***

In addition to regaining control of the business costs, it was also important to be vigilant as the attackers are inventive and may find different ways to combat and circumvent security mechanisms. If there is even a small pinhole in the platform security, the fraudsters will find it and exploit it.

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 opens up 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 Approov customers could - without requiring an app update - immediately see if their end users were running 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 Results

Integrating Approov into Papara's Android and iOS apps took 7 days after which the apps were released to the app stores and downloaded by customers. The Approov token check was simply monitored and not acted upon for another 21 days. This is the recommended approach in order to double check that everything is working as expected while waiting for the propagation of the new app versions across the installed base.

The Approov metric dashboards can be used to monitor Approov app authentication pass and fail data, as well as progress towards the required user installation percentage. Once the targets were reached, any API requests with no Approov tokens or with invalid tokens were blocked. Instantaneously, all phishing activities stopped and the vast majority of automated onboarding and transfers stopped, resulting in a dramatic drop in operating costs

Summary

Emre sums up his feelings about Approov:

> ***"We are very happy with Approov. It works well and matches exactly to the use cases we were initially concerned about. Having completed the integration and test in less than 30 days, we deployed the Approov protection and instantly saw the costs due to the fraudsters drop by 90%. Blocking so much fraudulent traffic from scripts and automators significantly lifts the pressure on Papara's systems as well as on our finances. 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