Investigation of Online Kerala Lottery

|  |  |  |  |
| --- | --- | --- | --- |
| **Category:**  Adversary Intelligence | **Industry**  Government | **Region:**  India | **Source:**  B2 |

# 

# Executive Summary

[CloudSEK](https://cloudsek.com/)’s contextual AI digital risk platform [XVigil](https://cloudsek.com/xvigil/) has discovered two applications that impersonate Directorate of Kerala state lotteries:

* Kerala Lottery Online
* India Kerala Lottery

These applications lure people into buying lottery tickets online. Threat actors are using referral links to spread their campaign. To prove legitimacy, threat actors show logos of government entities and create fake advertisements from accounts having 2,00,000+ followers on major social media platforms.

Further, threat actors have bought these domains -

* Upibank.com
* upibank.in
* indiacashpayment.com
* Ybbpay.net
* sliderummy.in

which act as payment gateway and allow threat actors to accept payments from major upi apps like (Gpay, Paytm, PhonePe, etc).

We discovered 6 UPI IDs each of a different entity out of which 5 are of yes bank and 1 of cosmos bank. We also discovered a strong connection between the applications developed in this campaign and the campaign of now banned Loan apps, In both campaigns *‘h5.domainname.tld*’ is used to host important content of the website which indicates that same group of threat actors or the same SDK is being used to create and launch such campaigns.

# 

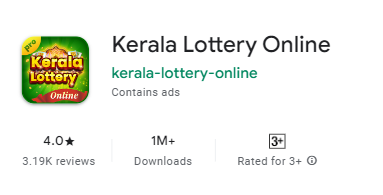
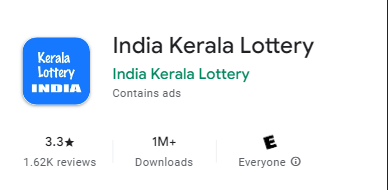
# Analysis and Attribution

[CloudSEK](https://cloudsek.com/)’s contextual AI digital risk platform [XVigil](https://cloudsek.com/xvigil/) has found below mentioned applications and websites posing as online kerala lottery and duping people of their hard earned money.

## Summary /Information on Campaign

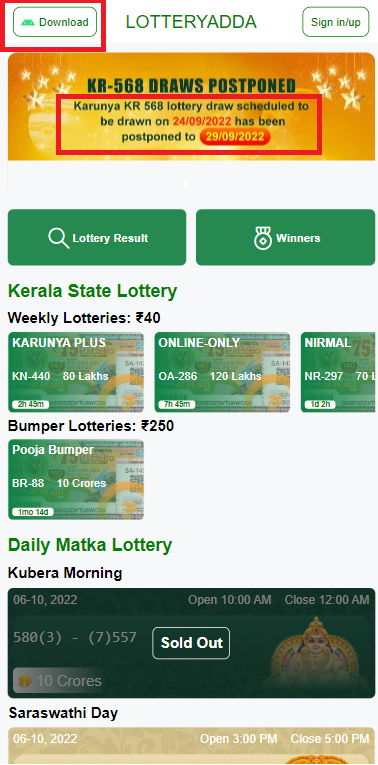
We discovered two applications hosted on Google Play Store impersonating the Online Kerala Lottery which operates in Offline mode.

* [Kerala Lottery Online](https://play.google.com/store/apps/details?id=com.lotteryonline.kerala)
* [India Kerala Lottery](https://play.google.com/store/apps/details?id=com.india.kerala.lottery&hl=en_US&gl=US)



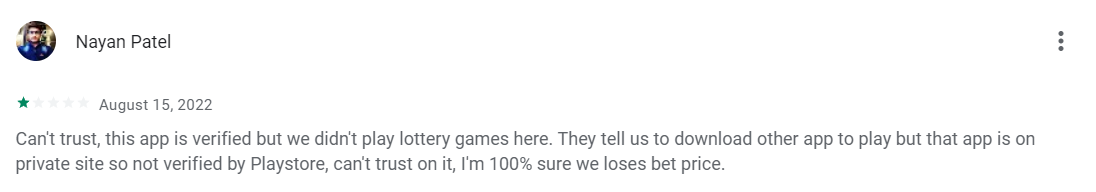
Applications listed on the playstore, both applications have over 1 Million downloads

* These applications allow you to purchase tickets for online gambling.

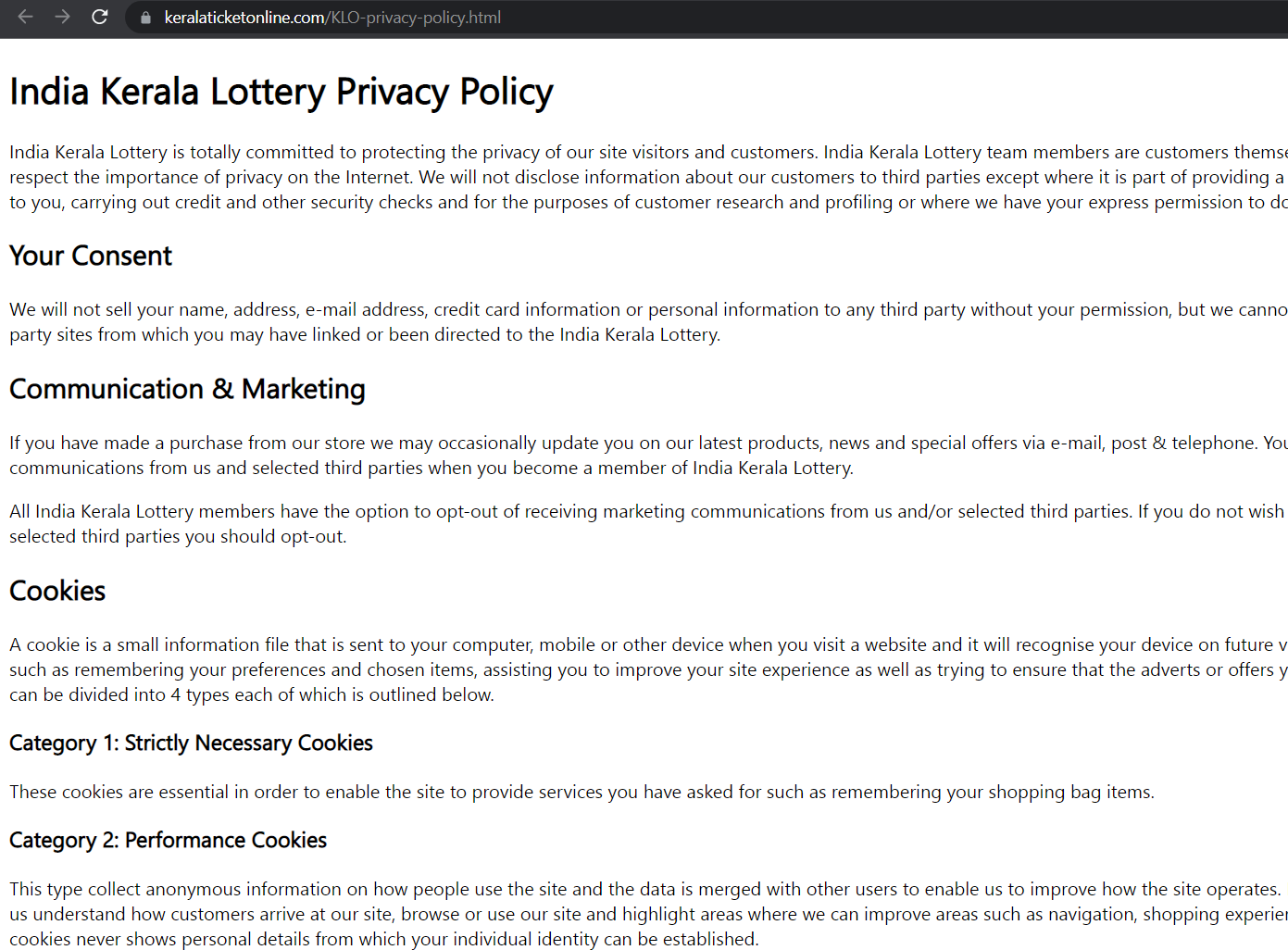


Home page of the application

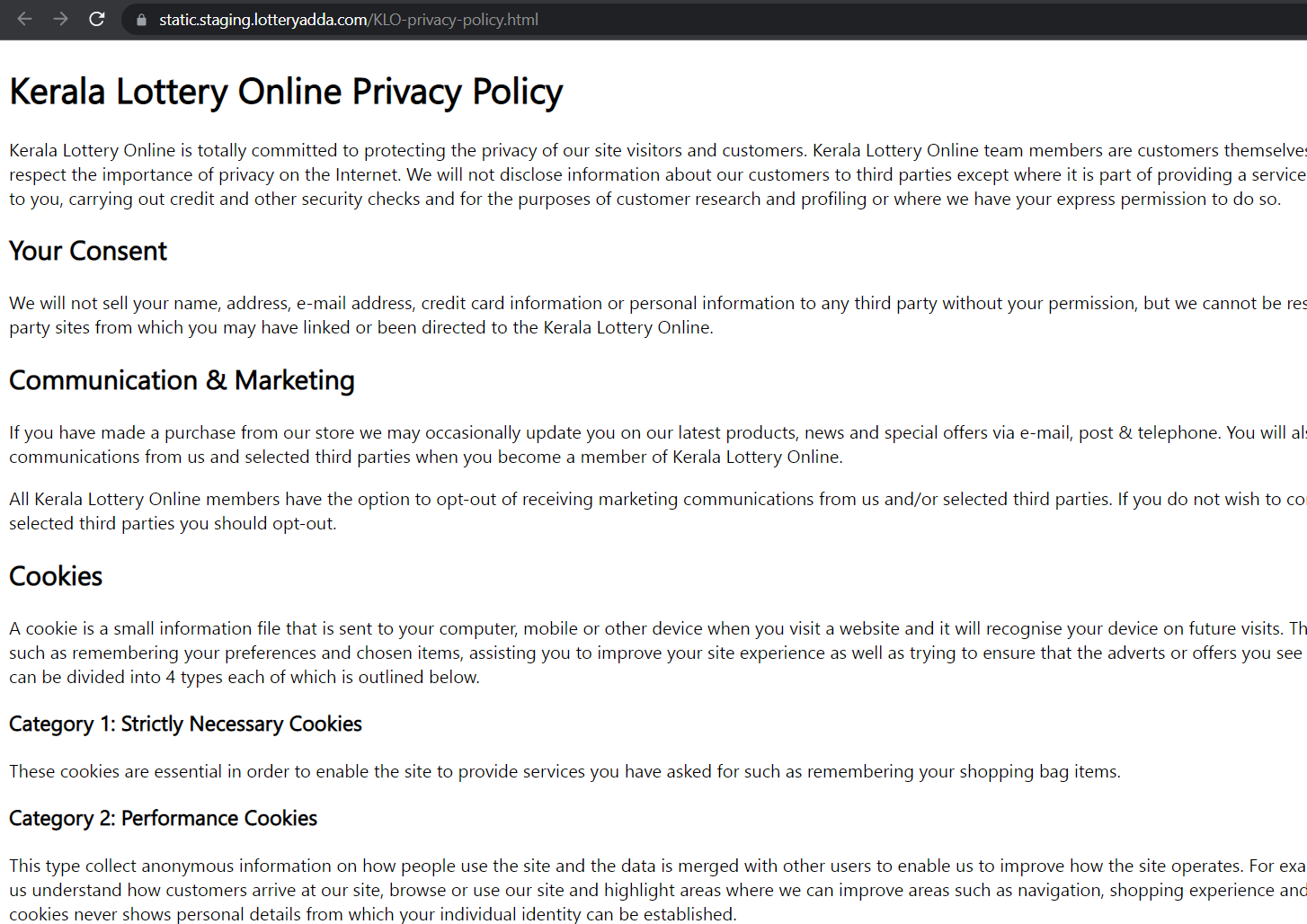
* Based on reviews posted on Google Play Store after successful installation of Lottery application from Google Play Store it prompts to install a secondary self-hosted APK file.



* We observed that both applications "Kerala Lottery Online" and “India Kerala Lottery” display the same privacy policy but operate under different names.



[India Kerala Lottery Privacy Policy](https://www.keralaticketonline.com/KLO-privacy-policy.html)

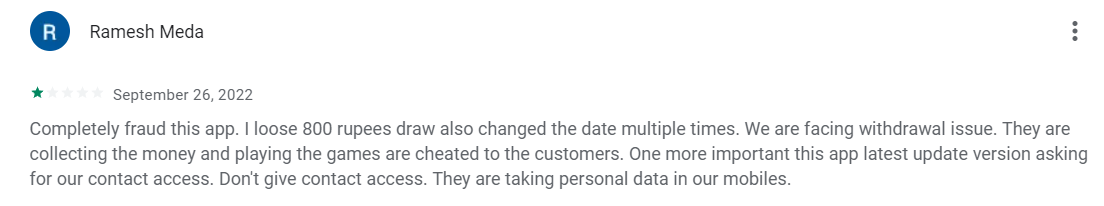


[Kerala Lottery Online Privacy Policy](https://static.staging.lotteryadda.com/KLO-privacy-policy.html)

Upon analysis of these two applications we discovered following email addresses were listed as developers contact:

* OnlineKeralaLotto@gmail.com
* sanjaykhankerala@gmail.com

Additionally, we discovered a review on Google Play Store, that suggests the application owners also postpone the draw dates which is mentioned in the second comment.



Review on google play store

* The applications ask for the following permissions,  
  Notable - Request to install packages (Required to install other applications on your device)



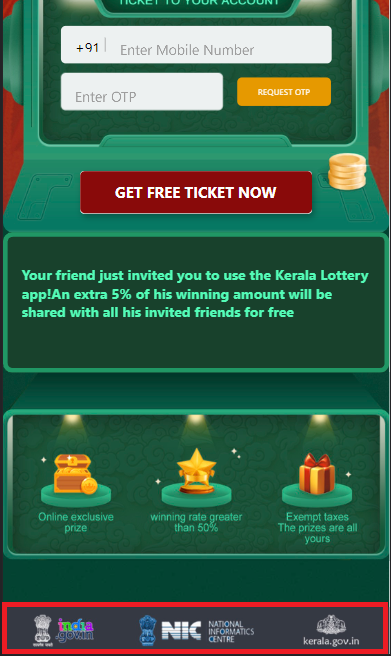
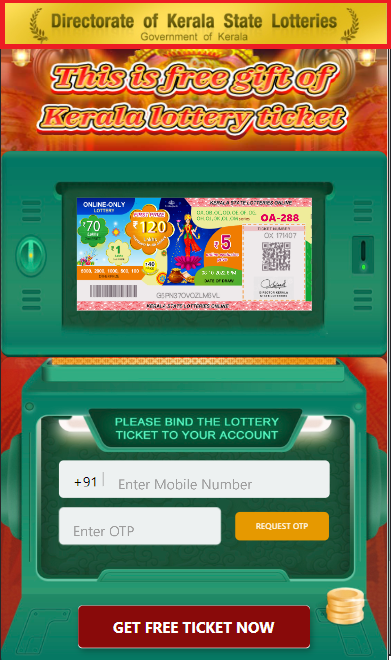
Permissions required by the application as shown on BeVigil

Detailed report on the applications

<https://bevigil.com/report/com.india.kerala.lottery>

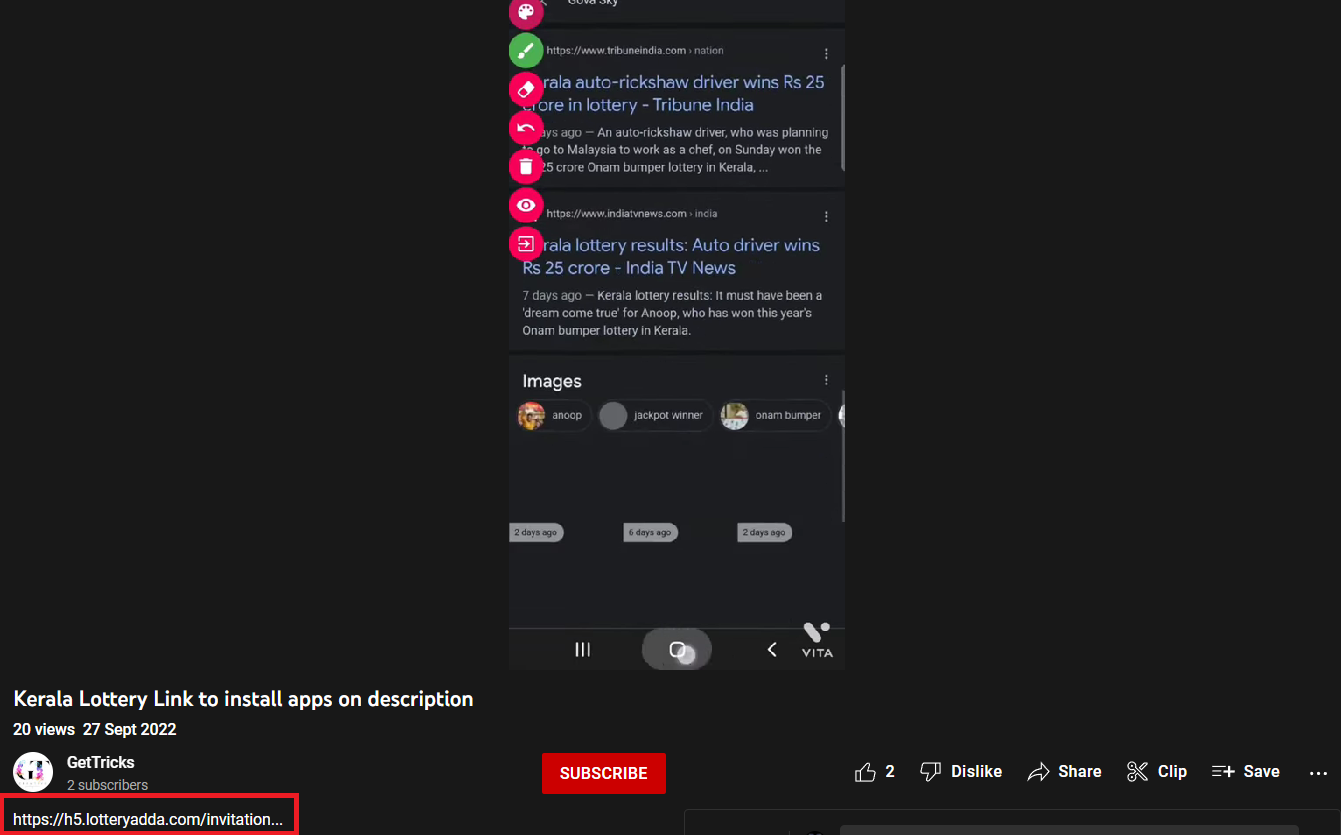
<https://bevigil.com/report/com.lotteryonline.kerala>

### Delivery Mechanism

* Threat Actors have used a referral program to spread their apps. Hence we were able to find multiple telegram groups, Youtube videos, Facebook and Twitter posts promoting the scam applications.
* This is the landing page of the referral link, wherein we can see threat actors mentioning 5% of the winning amount to be shared with all the users of the referral link and a free entry/ticket to the lottery.
* Logos of Directorate of Kerala State Lotteries, National Informatics Centre, Kerala State logo and India.  
  

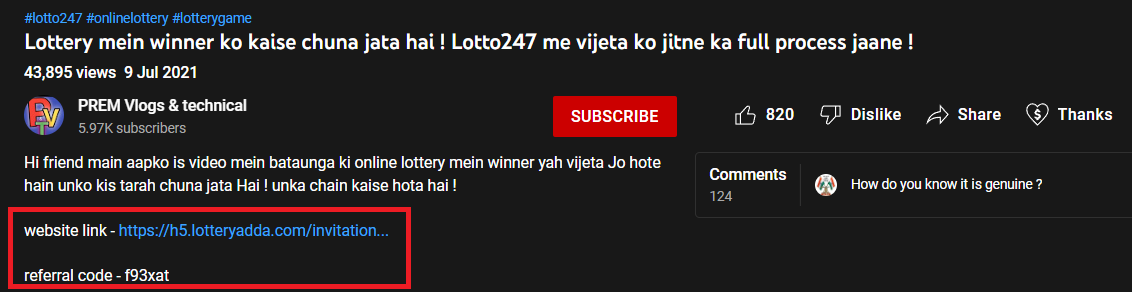
Landing page of the referral link showing logos of Directorate of Kerala State Lotteries, kerala.gov.in, NIC

* We also foundyoutube videos explaining the entire installation and usage procedure for the application. Referral link was also shared by the video uploader in the description of the video.

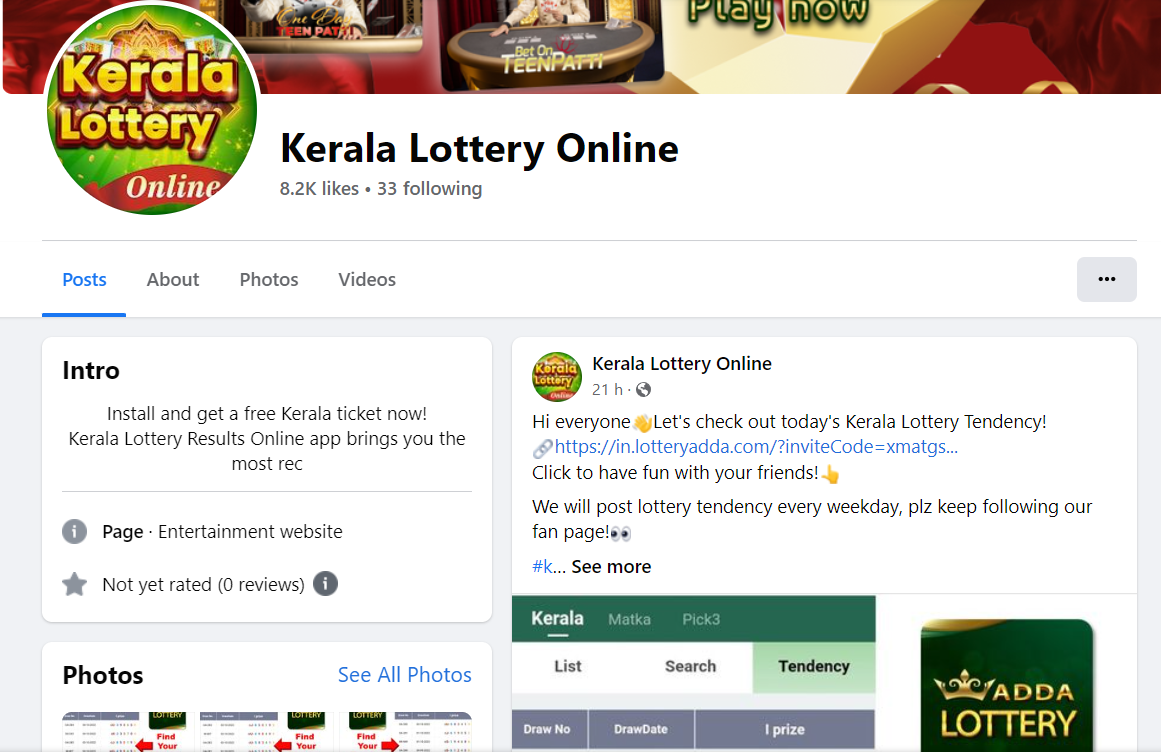


A youtube video with the referral link in the description

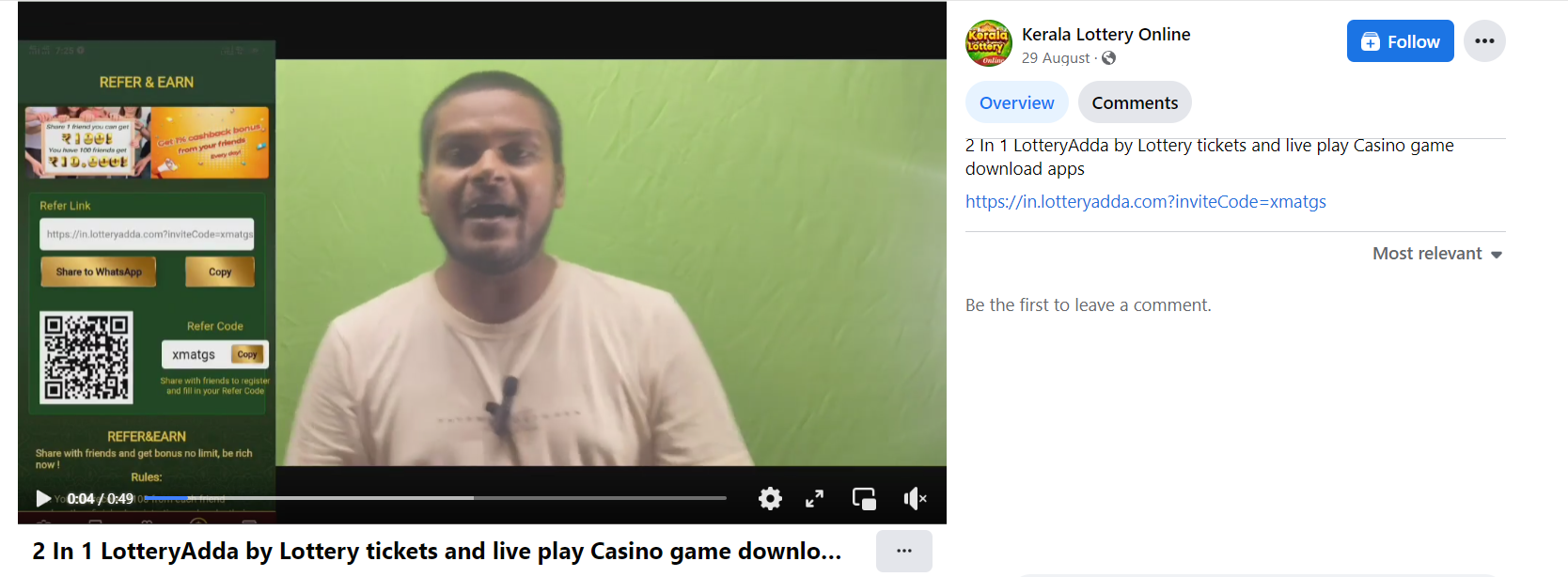
* This video explains a different international lottery game, but has a referral link to this campaign.



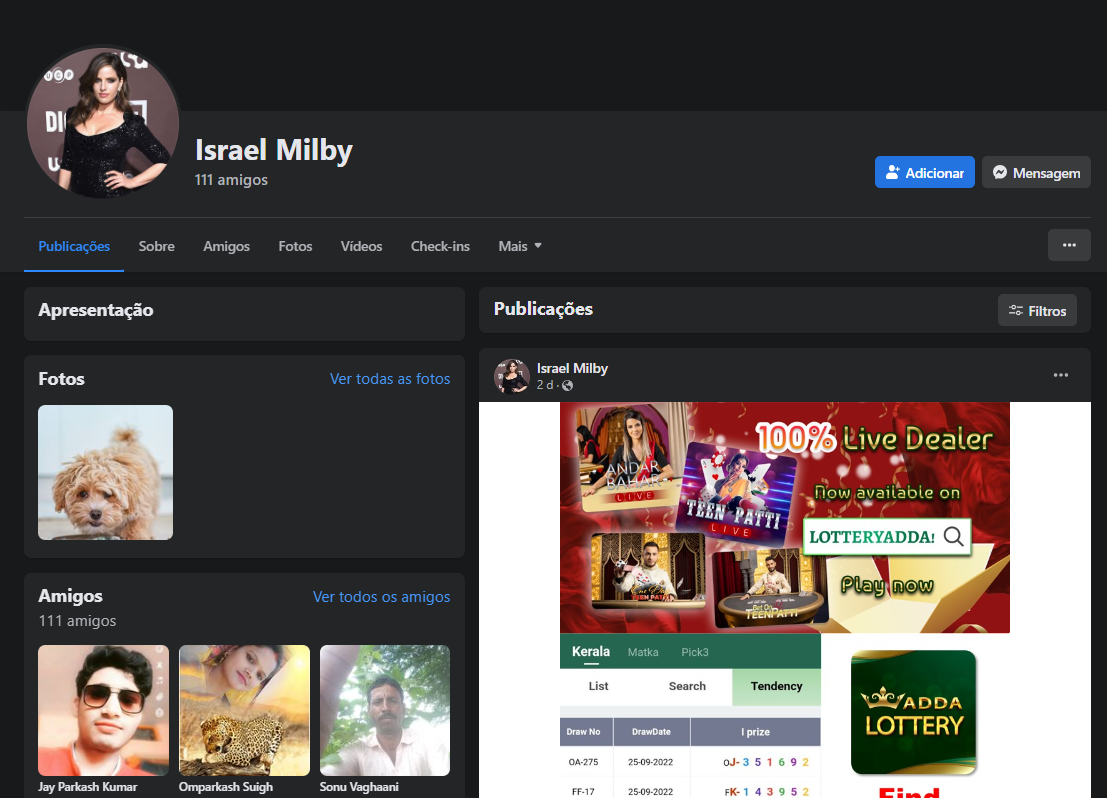
https://www.youtube.com/watch?v=ken8n8nUT60

* Page about the campaign made on facebook having 8.2k likes and 33 followers.

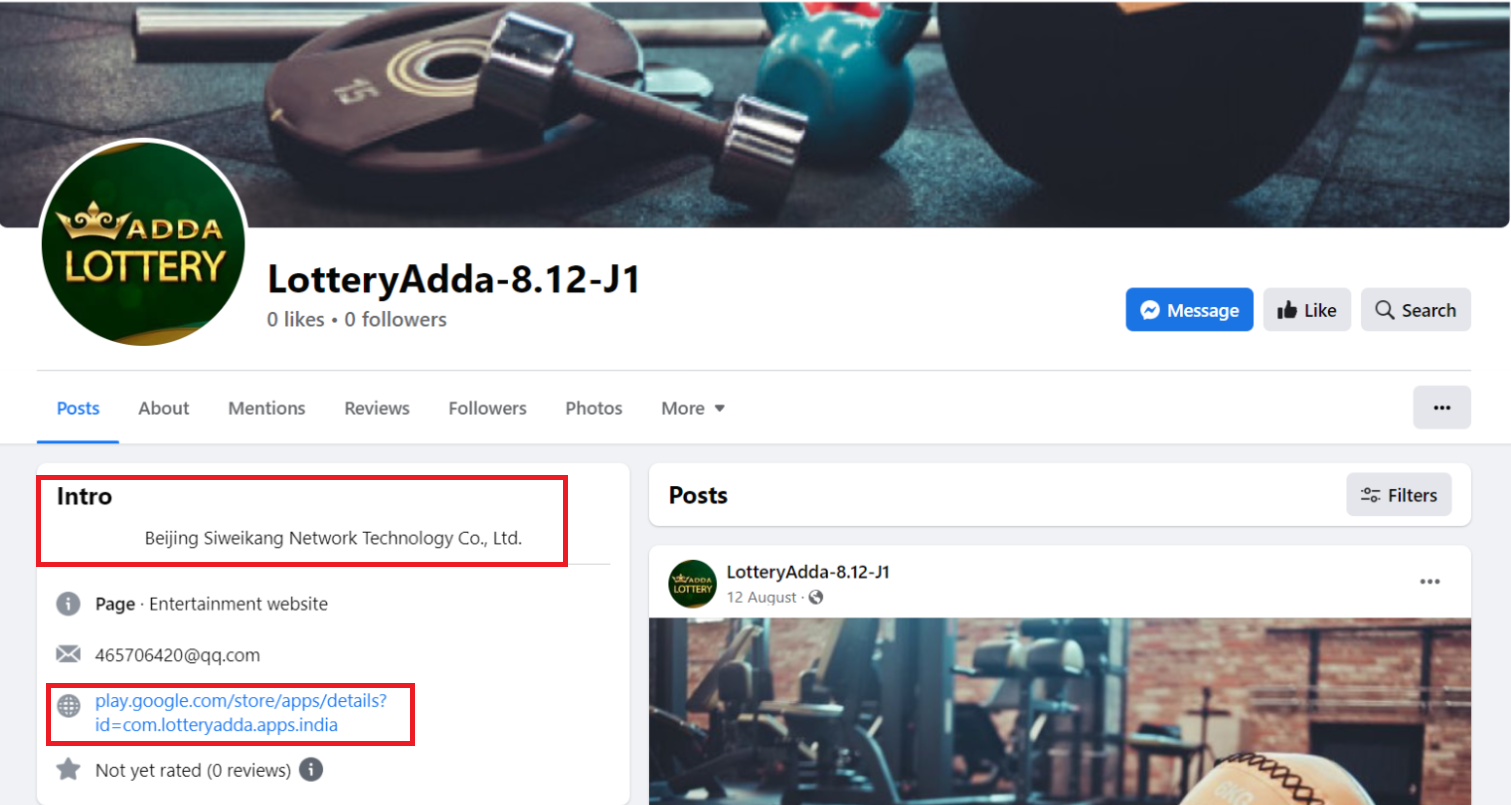
<https://www.facebook.com/people/Kerala-Lottery-Online/100083366756650/>

* Videos explaining about the application were also posted on facebook.

Advertisement on facebook

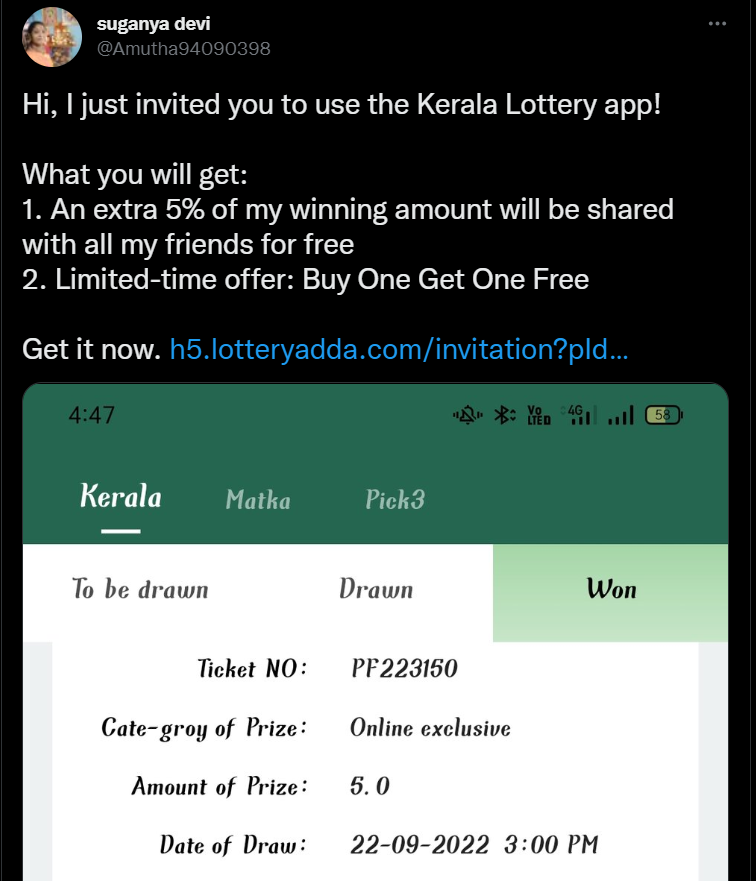
* Fake profiles on facebook using photos of hollywood actors are being created and used to advertise the application

Fake profile promoting the application

* We also discovered a facebook page which mentions a chinese entity, but no other mentions of the company were found on the internet.

A page with same name as application having chinese companies name and a now dead link to playstore

* Twitter account promoting the application, this profile has 2,00,000+ followers and has been promoting this application for over 6 months

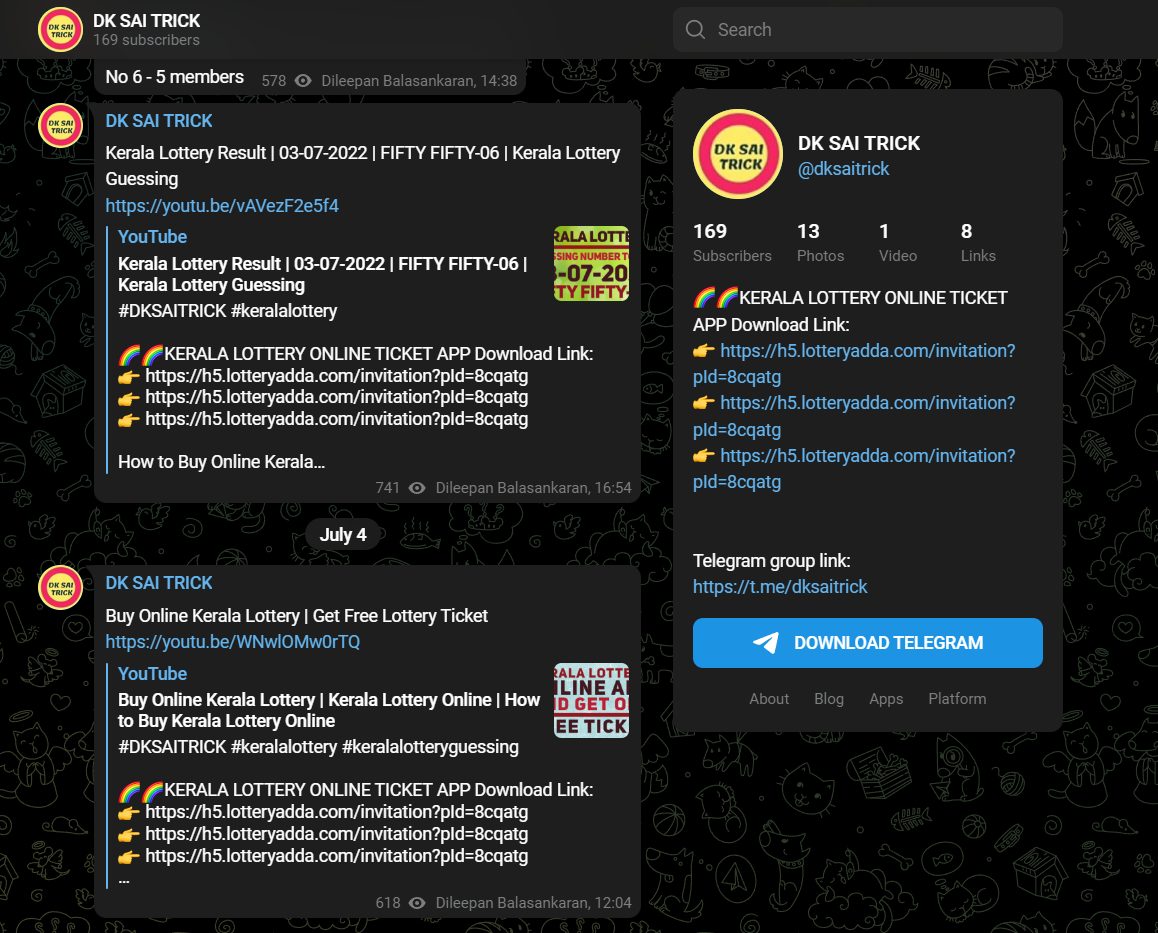


Twitter post advertising the application

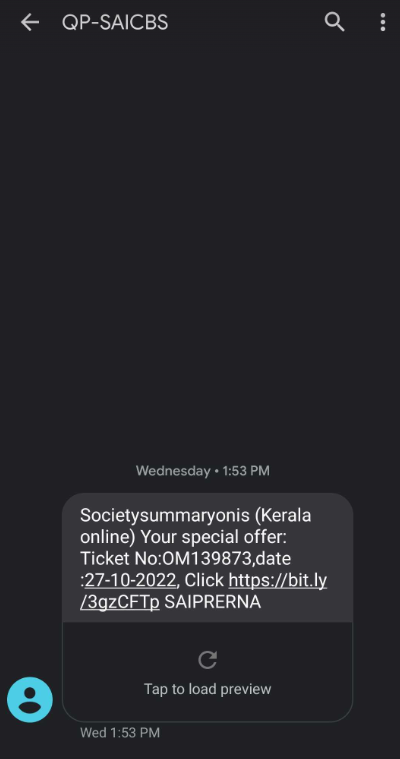


This account has 212.4K Followers and has promoted the app multiple times

* Telegram channel which has a long history of discussing and providing tips on offline lottery numbers is also promoting this application.



Telegram group advertising the application



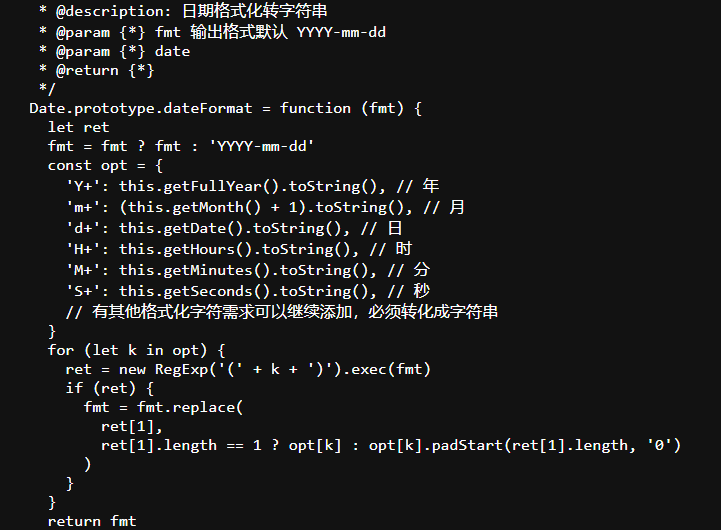
Threat actors also send SMS to invite users to buy tickets on the platform.

# Technical Analysis APK and Infrastructure

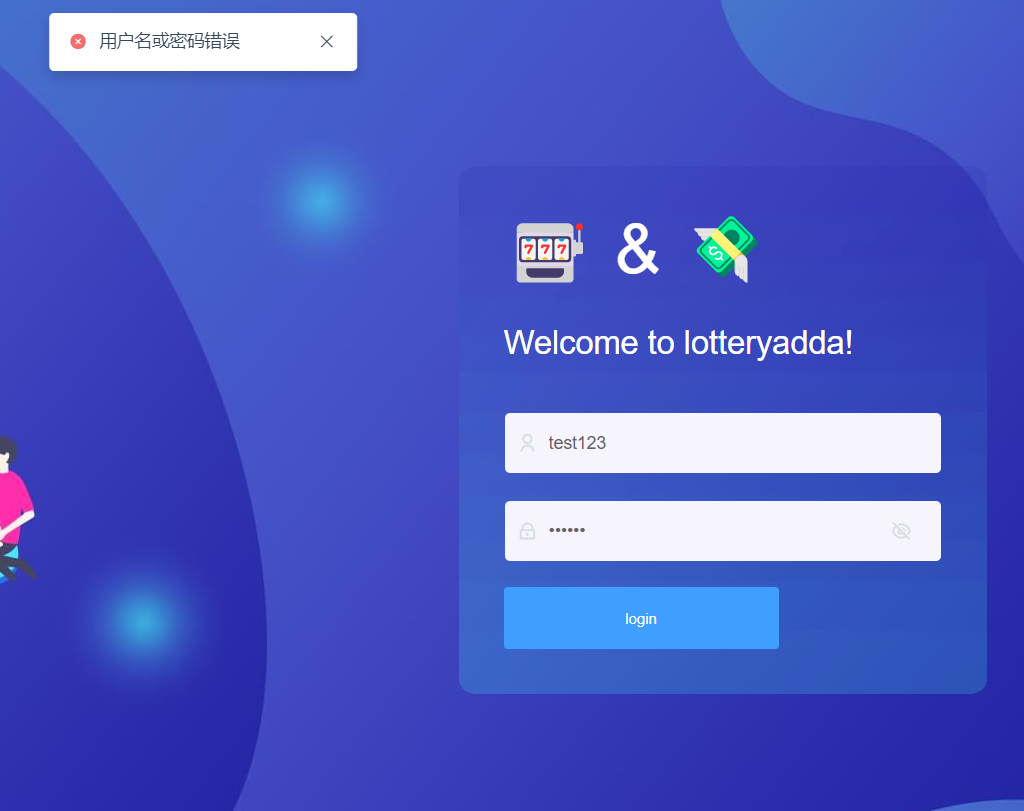
### Domain names owned by the group

* keralaticketone.com
* lotteryadda.com
* keralaticketonline.com
* lottomegawin.com
* kerala-ticket.com

Analysis of APK displayed Chinese characters but no significant attribution from China. Thus leading us to believe that a Chinese SDK must have been repurposed to develop the Android Application.



chinese characters in the source code of the website



Error generated on the website inchinese characters

**Infrastructure and Attribution on which the Application and Associated domains were hosted**

**IP addresses - Hosted on AWS, with an Elastic Load Balancer**

* 13.234.211.222
* 13.232.224.42
* 13.226.22.83

**Sub-domains of the group**

|  |  |
| --- | --- |
| * m.lotteryadda.com * static.lotteryadda.com * api.game.lotteryadda.com * h5.lotteryadda.com * dl.game.lotteryadda.com * in.lotteryadda.com * bapi.testing.lotteryadda.com * bapi.staging.lotteryadda.com * dl.lotteryadda.com | * www.lotteryadda.com * api.staging.lotteryadda.com * game.static.lotteryadda.com * lotteryadda.com * job.staging.lotteryadda.com * Admin.staging.lotteryadda.com * dl2.lotteryadda.com * Static.staging.lotteryadda.com |

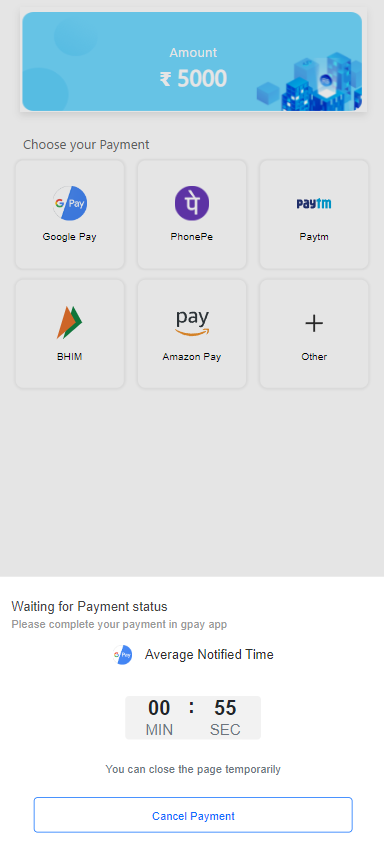
Subdomains associated with the group infrastructure

In the past, we have observed threat actors using the subdomain pattern with string h5[.]domain to host their content earlier in the report created by CloudSEK about banned loan applications titled “Investigation NPCI Onion Pay”. Hence we believe the threat actors could be of the same group or using the same SDK.  
  
H5 sub-domains in this campaign -

* h5.lotteryadda.com
* h5.keralaticketone.com
* h5.kerala-ticket.com
* h5.keralaticketonline.com

Other domains owned by the group - these act as the payment gateway url wherein the threat actors ask the users to pay via UPI.

* https://paymentupi.upibank.in
* https://dashboard.upibank.in
* https://pay.indiacashpayment.in



Payment gateway in the application

**UPI ADDRESS -**

|  |  |  |
| --- | --- | --- |
| **UPI ID** | **Company Name** | **Director Name** |
| gamecampipp@yesbank | Gamecamp Technologies Private Limited | - Kumbri Shailaja - GovindasamySathy |
| skenterprisesonline@yesbank | SK Enterprises | n/a - due to generic name |
| aeroglide@yesbank | Aero Glide India Private Limited | - Bhuvan Singh Gulati - Sandeep Kaur GulatiI |
| nineciytechnologiesipp@yesbank | Nine City Technologies Private Limited | - DilipDass - Martina Maria |
| byronipp@yesbank | Byrontec Solutions Private Limited | - GovindasamySathy - Sanjeev Govindasamy |
| airpay.techslidet266763@timecosmos | Tech Slide Technology Private Limited | - Shuvendu Biswas - Arajit Ghosh |

# 

# References

* **#**[Traffic Light Protocol - Wikipedia](https://en.wikipedia.org/wiki/Traffic_Light_Protocol)