****

**Dubious Apps On Google Play Store Impersonating Kerala Lottery**

**BENGALURU**: [CloudSEK](https://cloudsek.com/)’s contextual AI digital risk platform [XVigil](https://cloudsek.com/xvigil/) has discovered two applications that impersonate the Directorate of Kerala State’s lotteries -- Kerala Lottery Online and India Kerala Lottery.

These applications lure people into buying lottery tickets online. Threat actors are using referral links to spread their campaigns. To prove legitimacy, threat actors impersonate government entities and create fake advertisements from accounts having 200K+ followers on major social media platforms.

Both the applications hosted on Google Play Store have over one million downloads and were found impersonating the Online Kerala lottery which operates in offline mode. Logos of the Directorate of Kerala State Lotteries, National Informatics Centre, and Kerala State were used by the makers of the dubious apps. According to the Kerala lottery department, the state sells only paper lottery tickets and prohibits online sales.

**TECHNICAL DETAILS**

CloudSEK researchers found that both applications, "Kerala Lottery Online" and “India Kerala Lottery,” display the same privacy policy but operate under different names. Upon analysis of these two applications, the following email addresses were listed as developer’s contact: OnlineKeralaLotto@gmail.com and sanjaykhankerala@gmail.com. This indicates that the government entity is not operating the apps.

The applications ask for several permissions and notable among them was the request to install packages (Required to install other applications on your device).

The research shows a strong connection between the applications developed in this campaign, and previous campaigns targeting (now banned) Instant Loan Apps. In both campaigns, ‘h5.domainname.tld’ is used to host important content of the website, which indicates that the same group of threat actors or the same SDK is being used to create and launch such campaigns.

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.

**DISTRIBUTION NETWORK**

Threat Actors have used a referral program to spread their apps. There were multiple Telegram groups, YouTube videos, Facebook and Twitter posts promoting the scam applications.

On the landing page of the referral link, threat actors can be seen 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.

YouTube videos explaining the entire installation and usage procedure for the application were also found. Referral link was also shared by the video uploader in the description of the video. The video explains a different international lottery game, but has a referral link to this campaign.

Fake profiles on Facebook, using photos of Hollywood actors, are being created and used to advertise the application. The Twitter account promoting the application has 200K+ followers, and has been promoting this application for over 6 months.

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

“Cashing on the popularity of Kerala lottery, threat actors have created multiple apps and websites to sell tickets and conduct lotteries which is banned by Kerala state government. To get more users, threat actors promote their apps on various social media platforms, along with WhatsApp and Telegram groups. Several websites have also been created to promote the apps and make the apps look legitimate,” said a CloudSEK researcher.

**SAFETY MEASURES**

-        It is advised to buy lottery tickets from government-authorized stores. As per Kerala state rule, only physical tickets are permitted for sale.

-        Refrain from participating in online Kerala Lottery as conducting online Lottery is banned in Kerala.

-        Avoid downloading dubious apps, as it may compromise users’ critical information.

**About CloudSEK**

Singapore-headquartered CloudSEK is a contextual AI (Artificial Intelligence) company, founded in 2015, by cybersecurity expert Rahul Sasi, with the aim to construct a future where intelligent machines can emulate human cognition to predict cyber threats even before they occur.

CloudSEK’s central proposition is to leverage AI to build a rapid and reliable detection, analysis, and alert system that offers swift detection across internet sources, precision analysis of threats, and prompt resolution with minimal human intervention.

CloudSEK offers the power of Cyber Crime monitoring, Brand Monitoring, Attack Surface monitoring, and Supply Chain Intelligence to give context to customers’ digital risks. CloudSEK’s single unified dashboard allows customers to triage and visualize all their digital threats in one place. CloudSEK also offers workflows and integrations to manage and remediate the identified threats.