Ministry of Education
Government of India

G20 भारत 2023 INDIA

Azadi Ka Amrit Mahotsav

विद्यया ऽ मृतमश्नुते
एन सी ई आर टी
NCERT

Indian Cyber Crime Coordination Centre

Online training on

Internet of Things (IoT) and Mobile Security

Organized by CIET-NCERT in collaboration with I4C, MHA

7 Sep, 2023 **4:00 pm-5:00 pm**

Day 4: Mobile: Security, Threats and Safety Measures

Dr. Deepak Kumar
Sr. Cyber Intelligence and Digital Forensic Professional
I4C, MHA

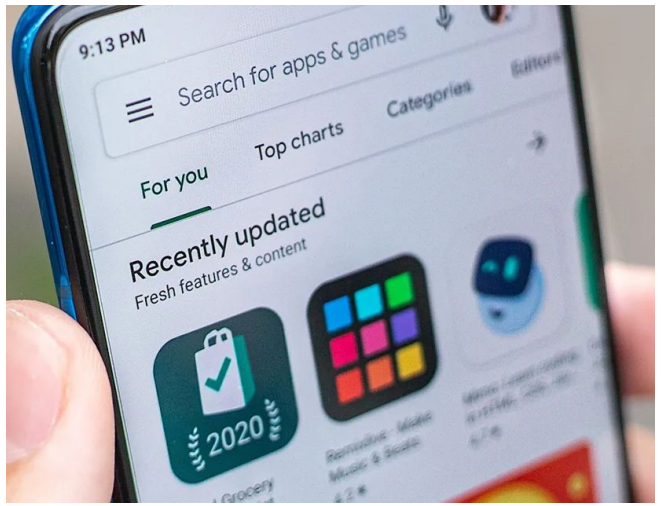
Mr. Shinku Saran Singh
Deputy Commandant
I4C, MHA

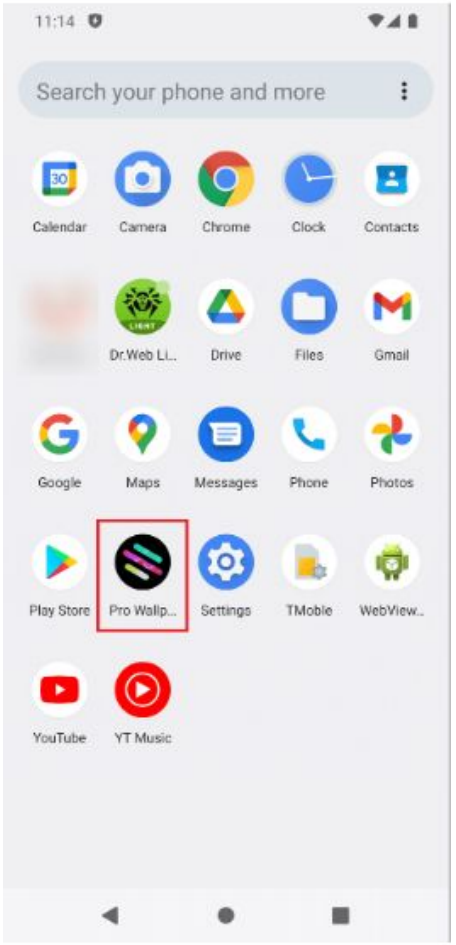
Shifted from vishing to mobile app

Ministry of Education
Government of India
सत्यमेव जयते

Indian Cyber Crime Coordination Centre

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
सत्यमेव जयते





MOBILE THREATS

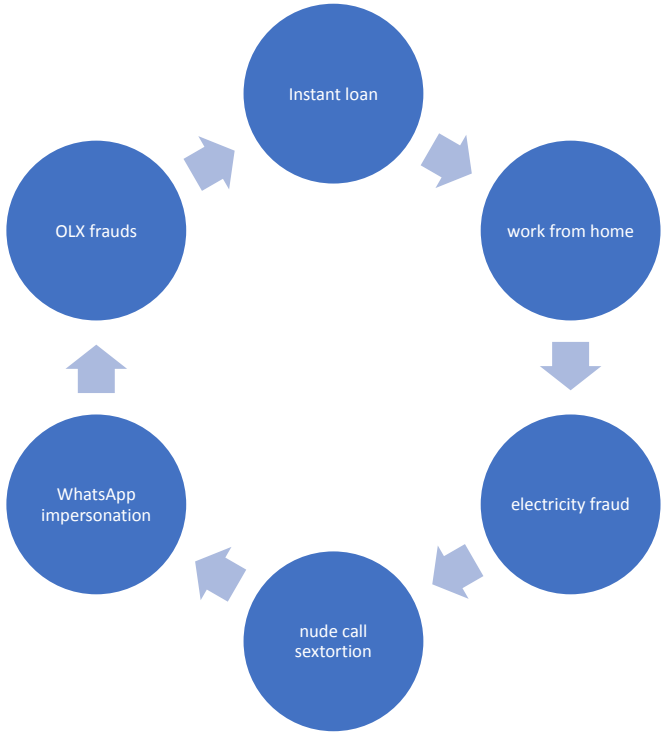
Threat actors are using newly discovered "SandStrike spyware" and delivered via a malicious VPN application to target Android users https://www.bleepingcomputer.com/news/security/new-sandstrike-spyware-infects-android-devices-via-malicious-vpn-app/ Nov 2022

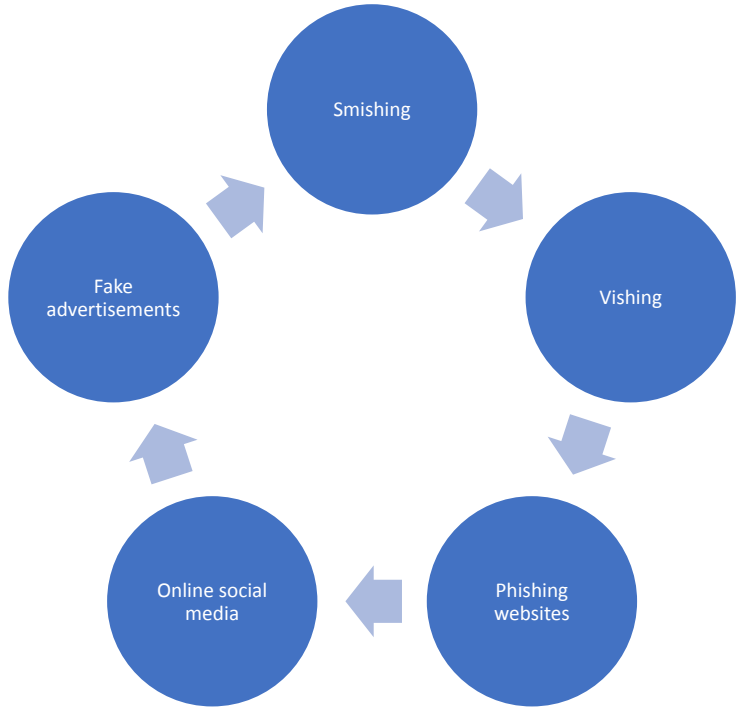
New ERMAC 2.0 banking Android Trojan malware steals accounts, wallets from 467 apps to steal account credentials and crypto wallets. https://www.bleepingcomputer.com/news/security/new-ermac-20-android-malware-steals-accounts-wallets-from-467-apps/ May 2022

Meta uncovers 400 malicious apps on Android and iOS apps, Fraudsters are stealing Facebook users' information through malicious apps downloaded from Apple and Google's software stores https://www.scmagazine.com/analysis/application-security/meta-uncovers-400-malicious-apps-on-android-and-ios-apps Oct 2022

Experts Uncover 85 Apps with 13 Million Downloads Involved in Ad Fraud Scheme https://thehackernews.com/2022/09/experts-uncover-85-apps-with-13-million.html?m=1 Sep 2022

RED FLAGS





- The first stage of gathering contacts could by followed by mass-phishing via text messages.
- Fake e-commerce websites, phishing campaigns, data & credential harvesting
- Fake SMS Headers & Bombers contains short links of WhatsApp example: wa.me/919560348xxx
- Domains mimicking (look alike, name and logo) popular Android app and services, brands

METHODOLOGY

- Furnished in many folds Instant loan, work from home, electricity fraud, nude call sextortion, WhatsApp impersonation, etc.
- Propagating through Smishing, Vishing, Phishing of online social media websites and Luring by fake advertisements
- The first stage of gathering contacts could by followed by spear phishing via text messages.
- URL shared through telegram channels, groups, referral
- If they download the app, they are met with a permission request that demands complete control of their device.
- Designed to run silently in the background, constantly spying on its victims without raising suspicion

Loan App

Dating App

Gaming App

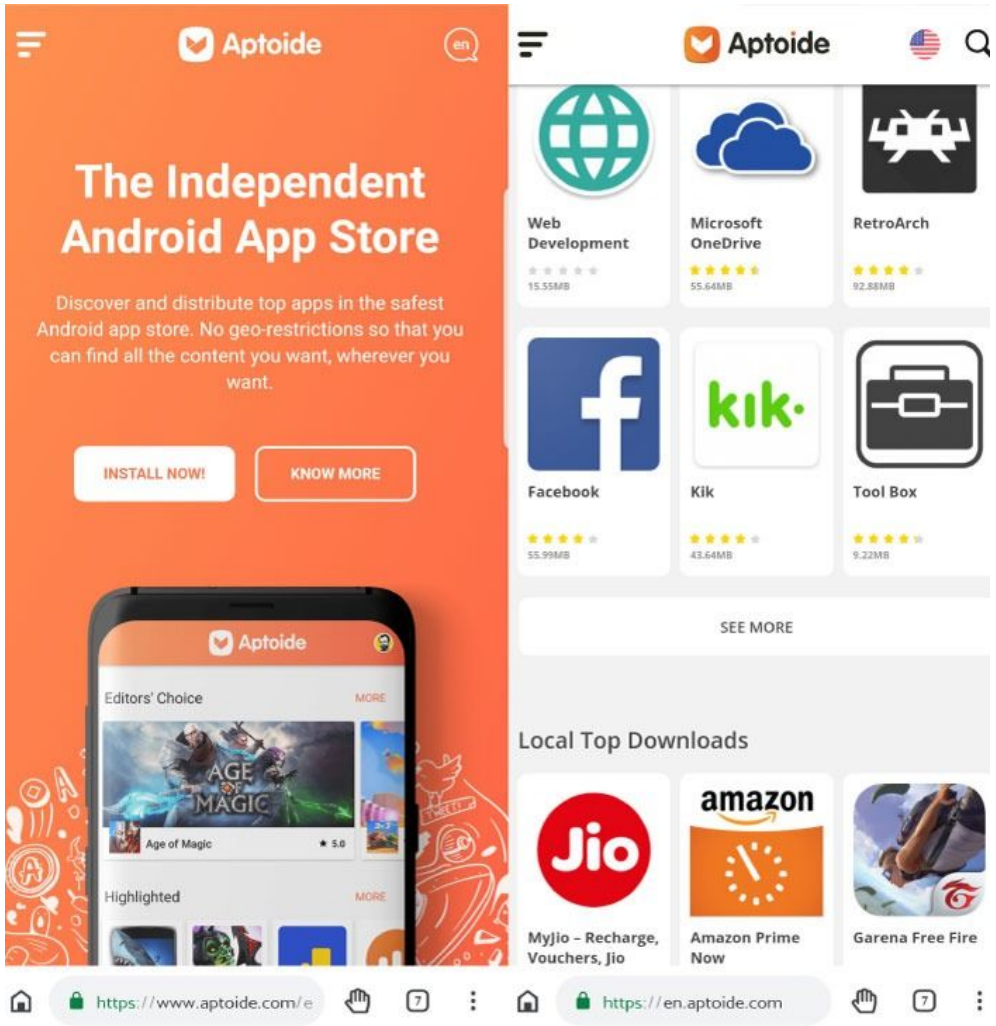
Screen Sharing / Remote Access Apps

Covid-19 Apps

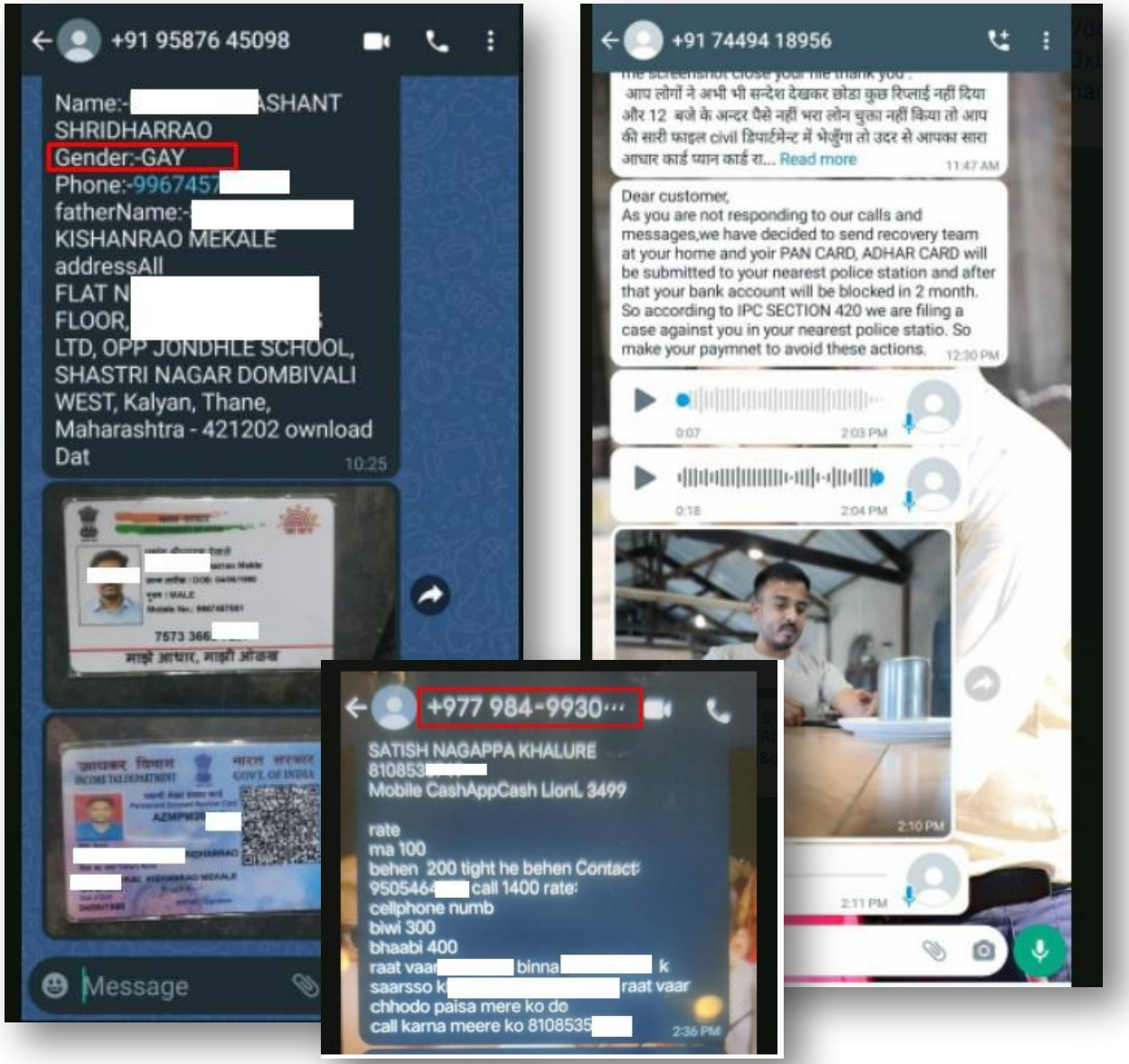
E-Shopping Apps

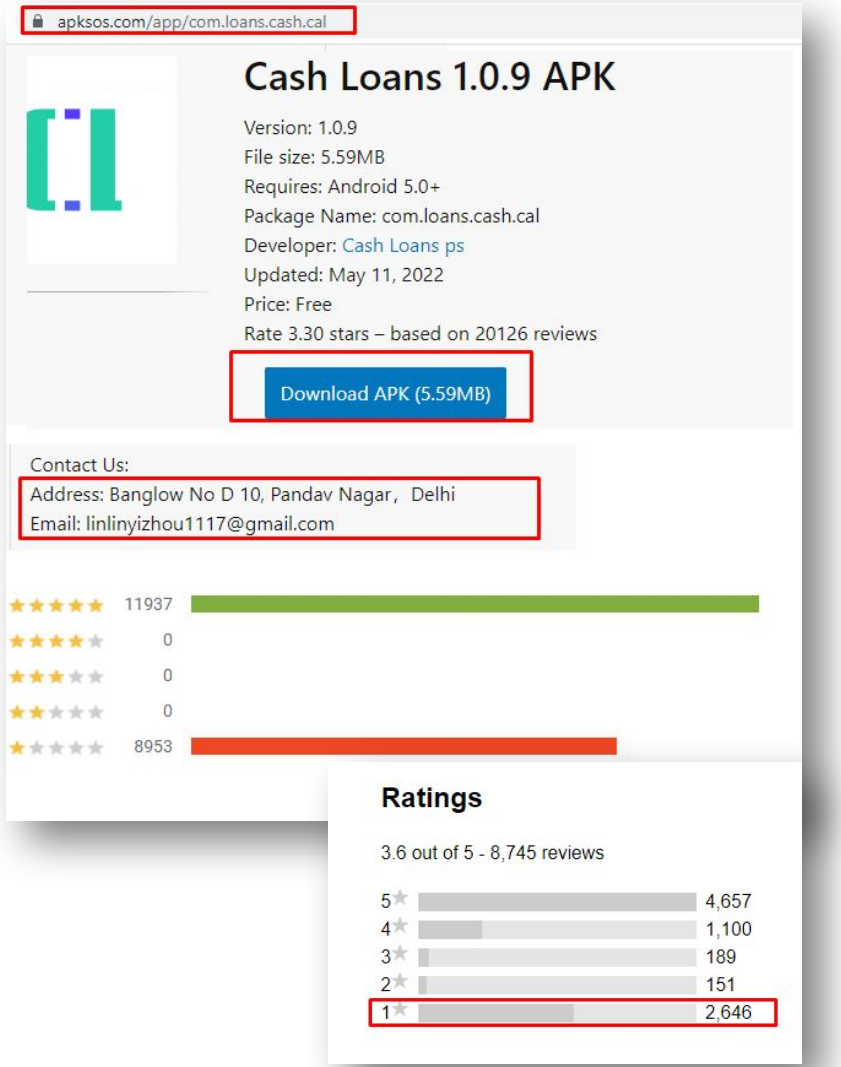
Social Media Apps

Unknown / Unverified (Fake) Apps

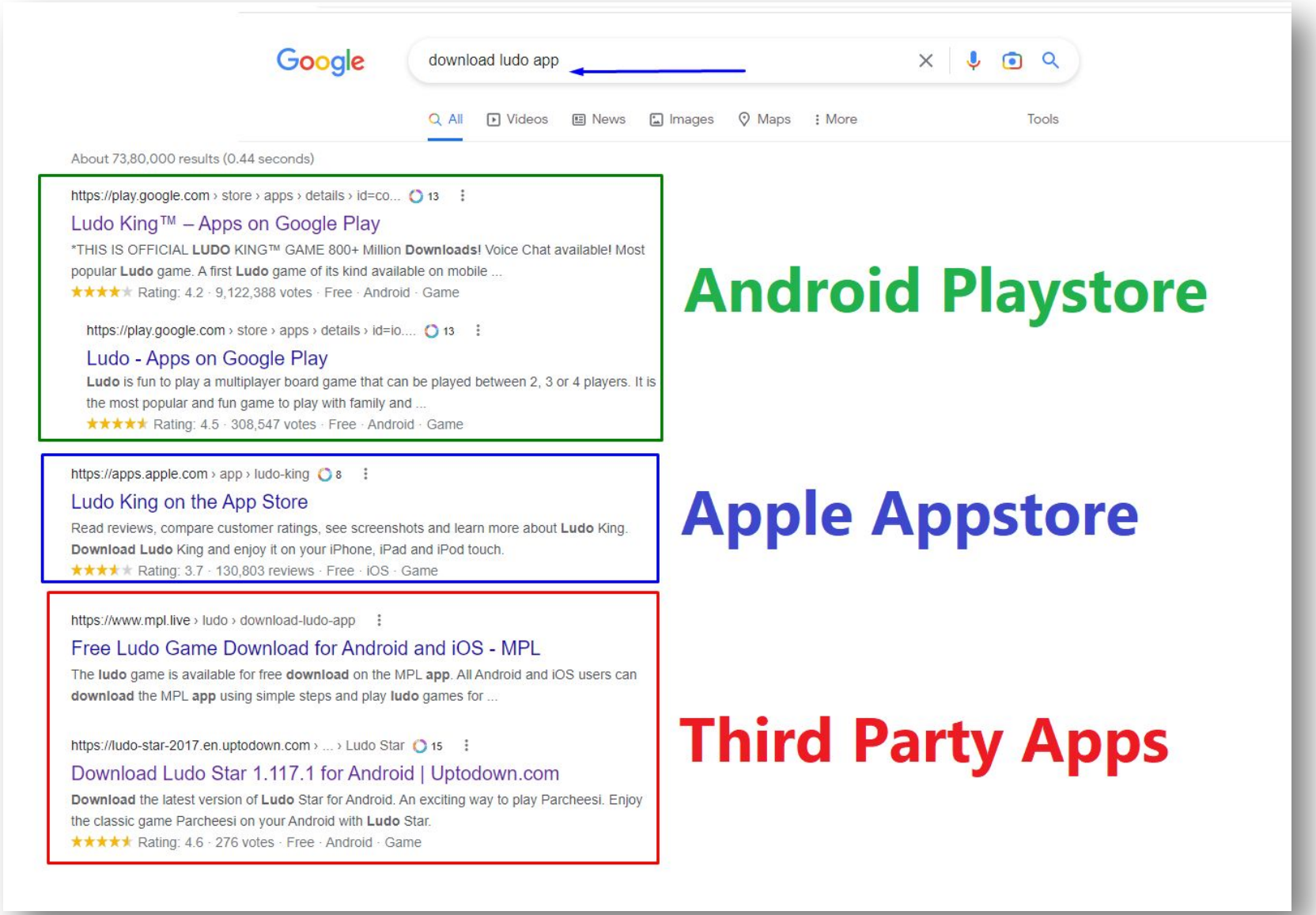


Loan App Frauds

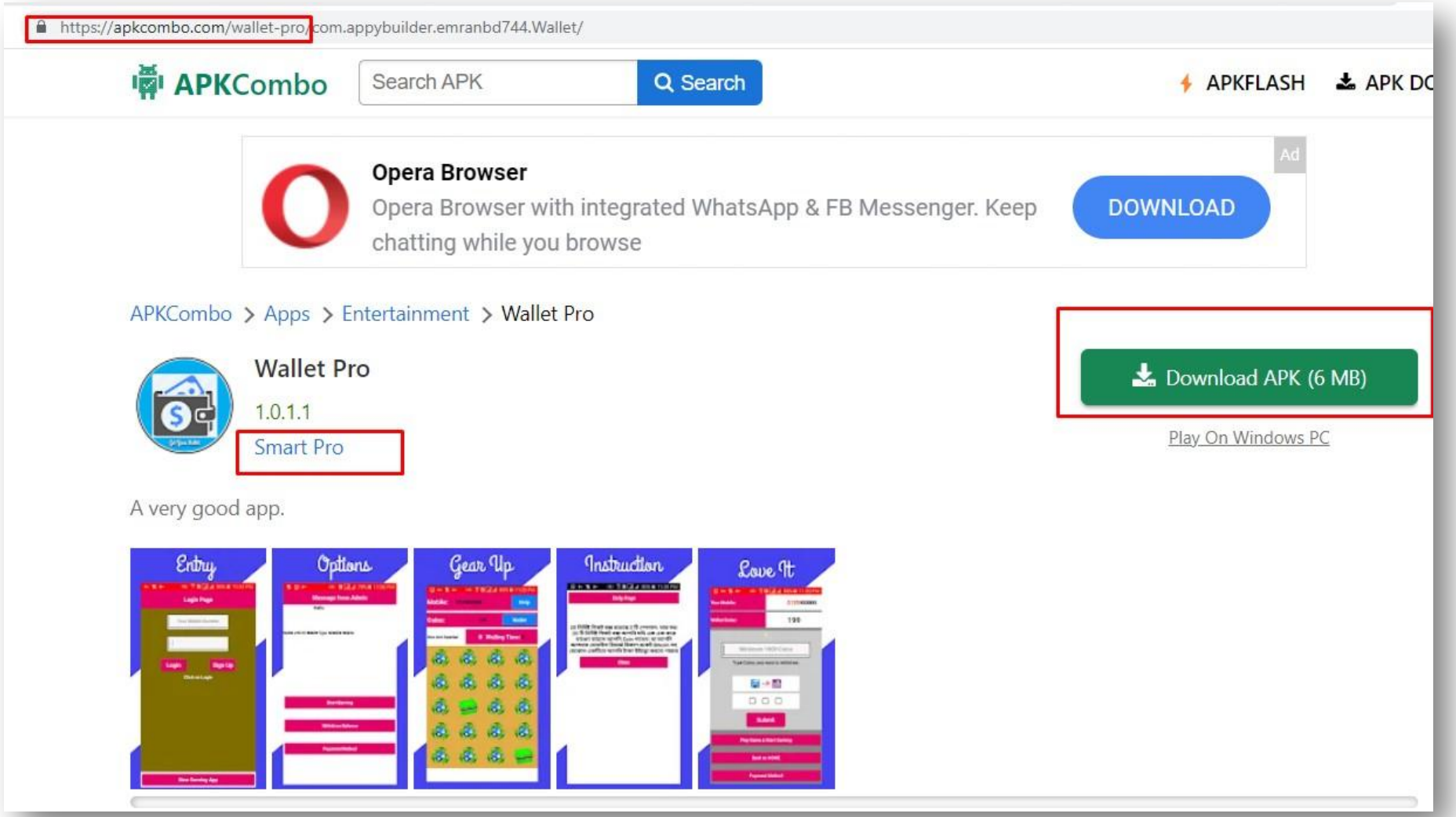




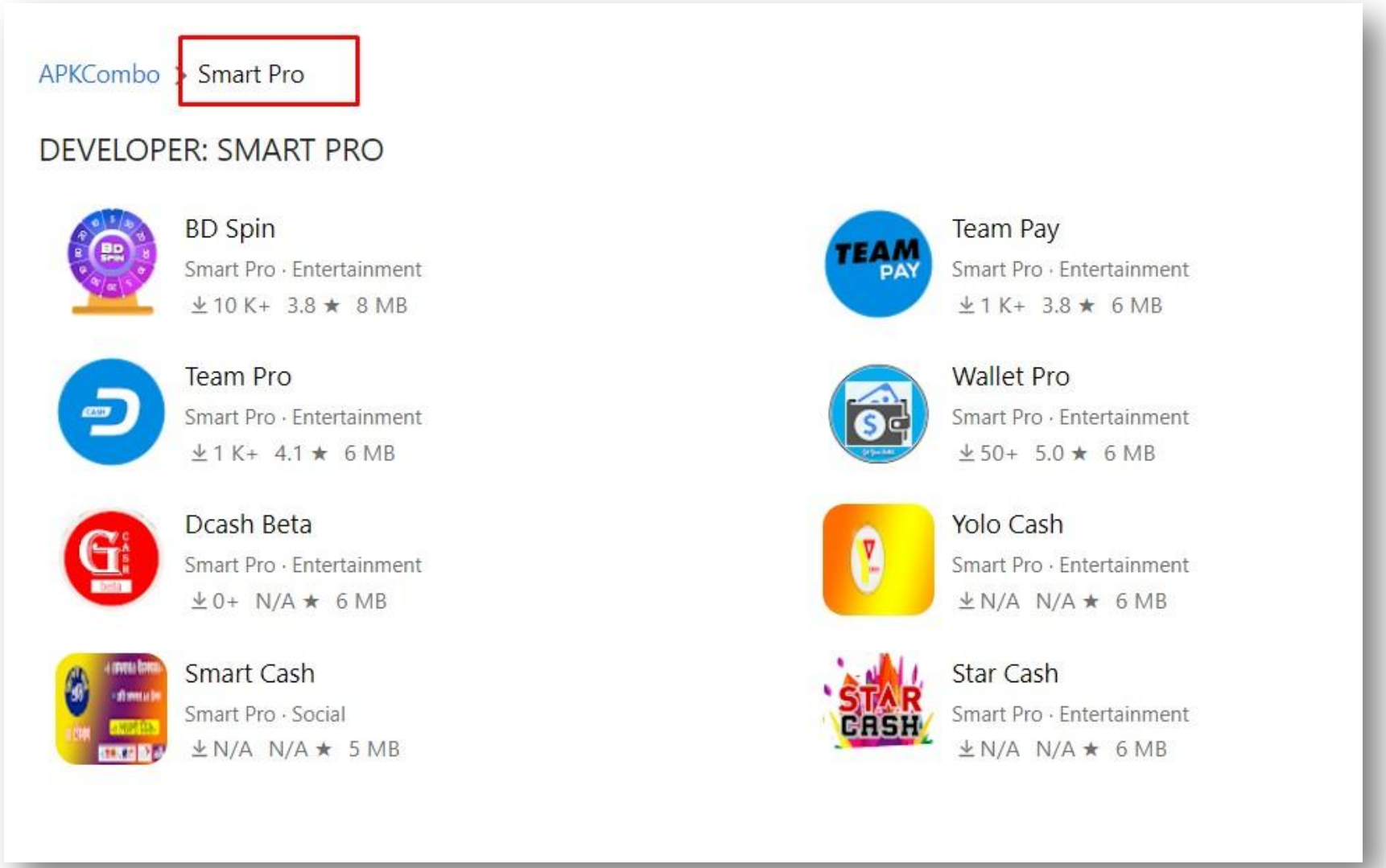
MOBILE APPLICATIONS



Third Party Apps

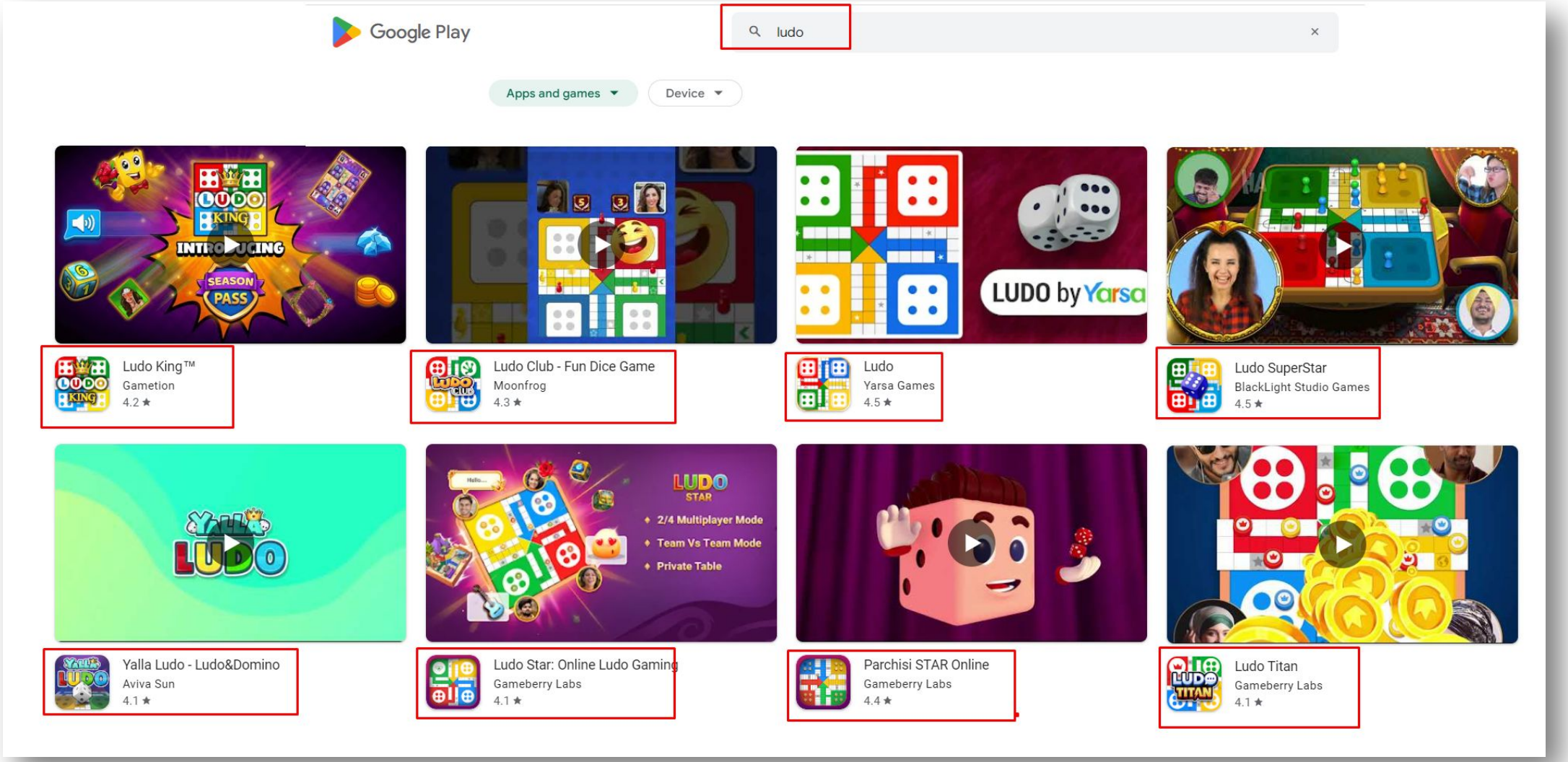


Third Party Apps



EXAMPLE 1

Understand the mobile app

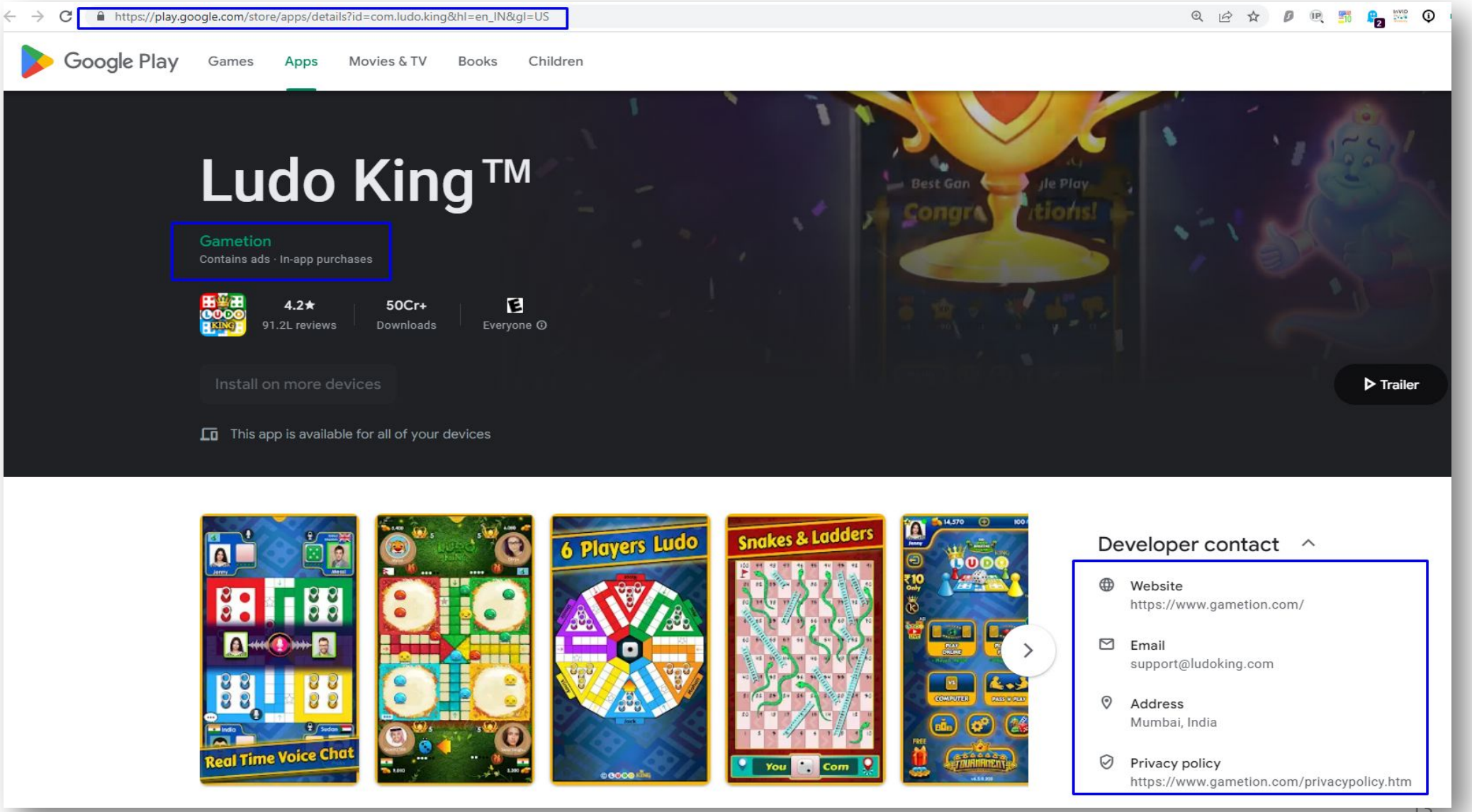


Scenario 1

Ministry of Education
Government of India
सत्यमेव जयते

Indian Cyber Crime Coordination Centre

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
सत्यमेव जयते



Scenario 2

Ministry of Education
Government of India
सत्यमेव जयते

Indian Cyber Crime Coordination Centre

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
सत्यमेव जयते

https://play.google.com/store/apps/details?id=com.ludo.ludoapp&hl=en_IN&gl=US

Google Play Games Apps Movies & TV Books Children

Yal3ab Ludo

pirateking
Contains ads · In-app purchases

50T+
Downloads

Teen

Install

Add to wishlist

This app is available for all of your devices

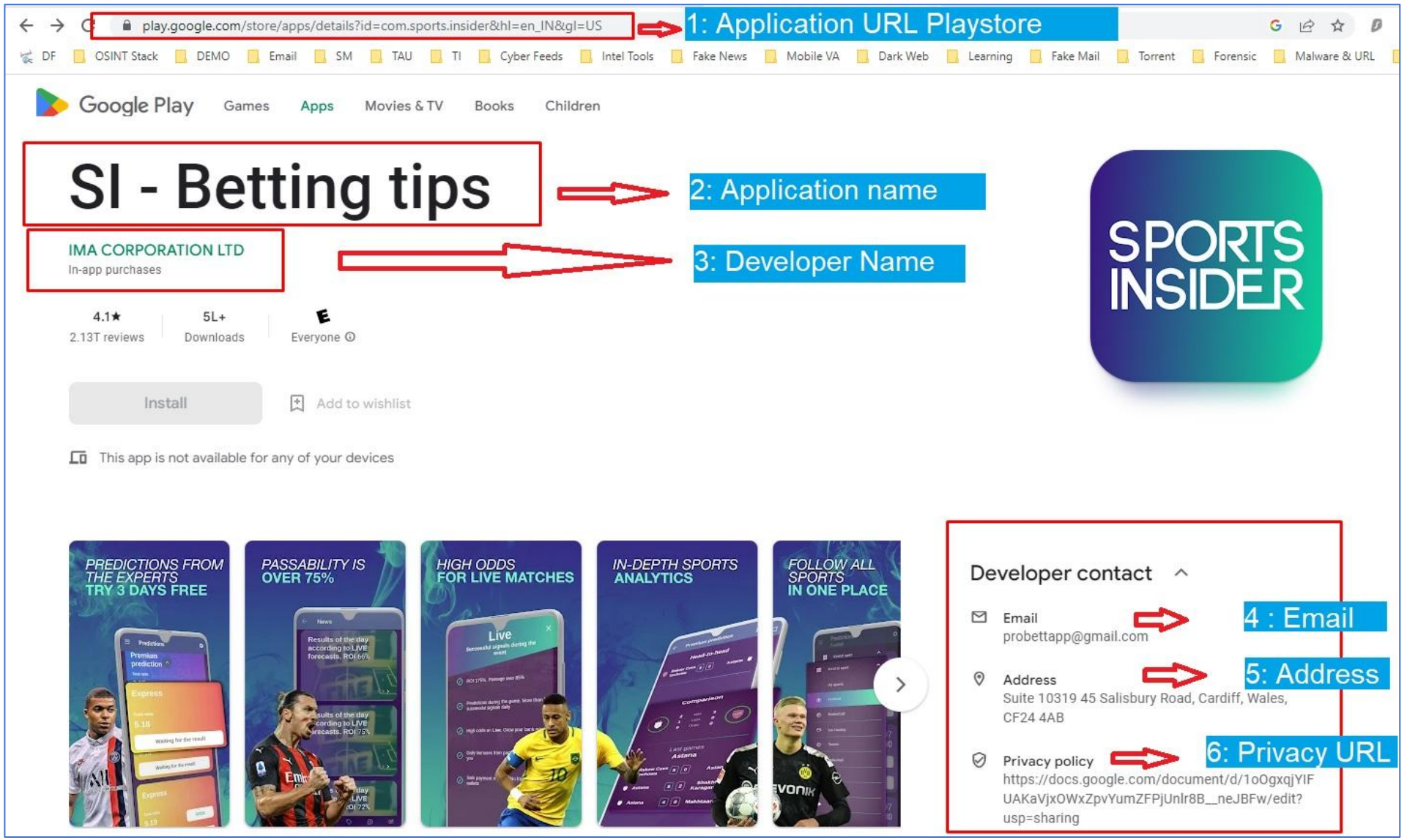
Developer contact

Email
bloodforest9@gmail.com

Address
BEIJING SHI CHAO YANG QU BEI TU CHENG DONG LU 1 HAO LOU 2 CENG 3003 SHI

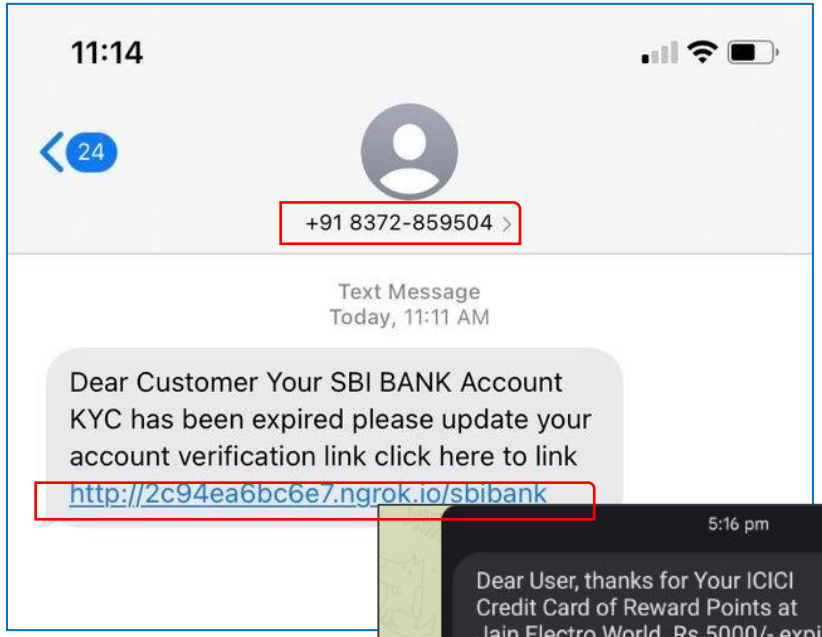
Privacy policy
https://dl.pokersky.net/yal3ab_ludo/privacy_policy.html

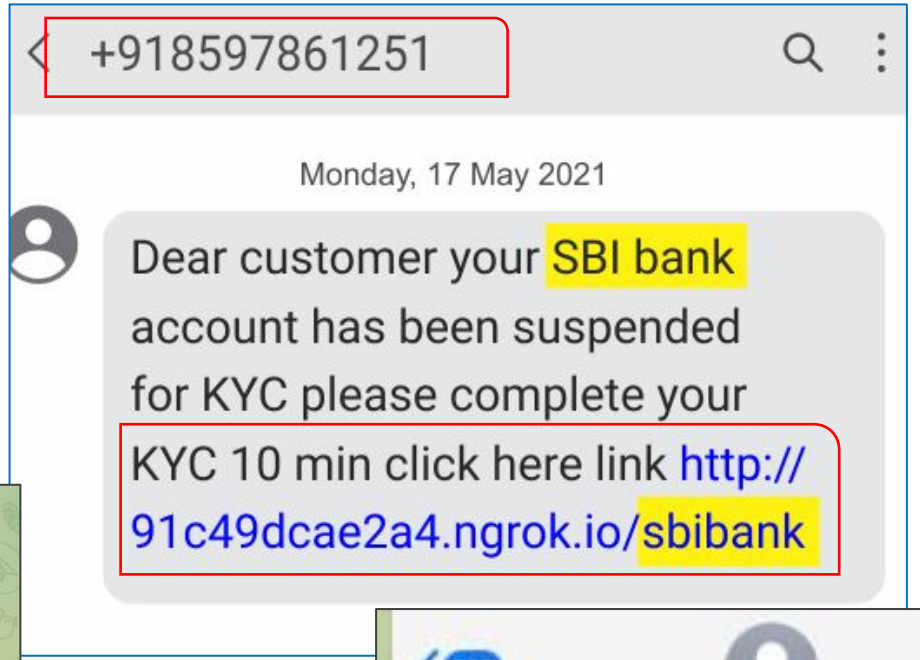
Observation

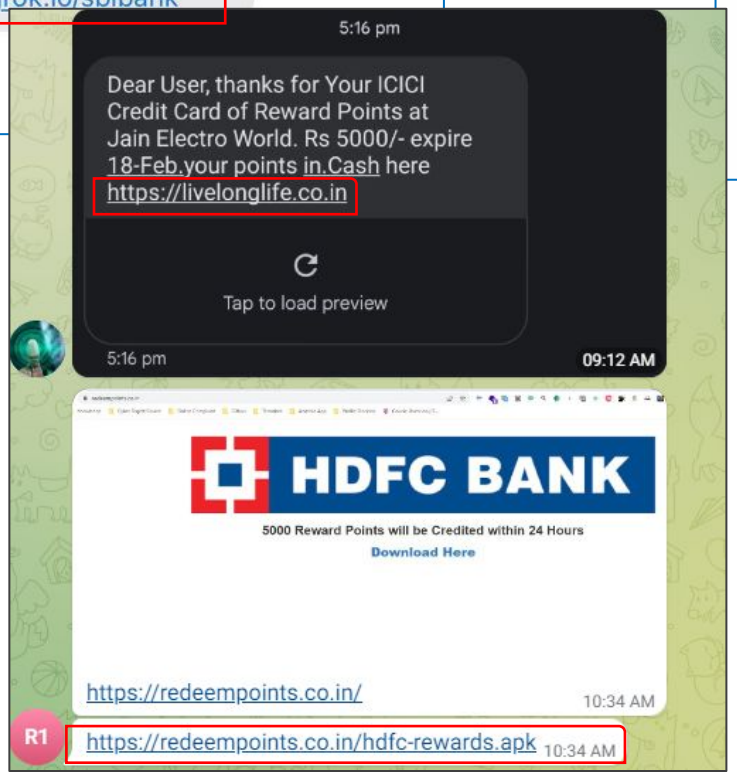


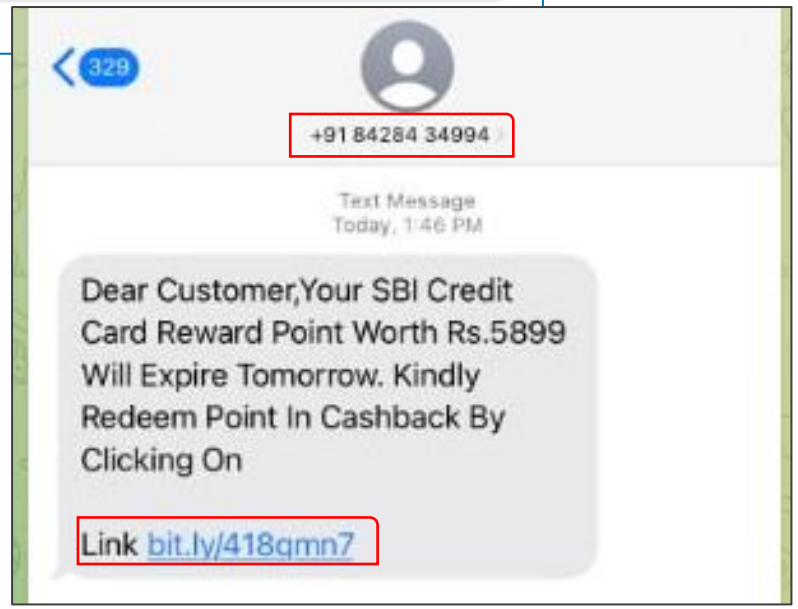
EXAMPLE 2

ATTACK METHOD

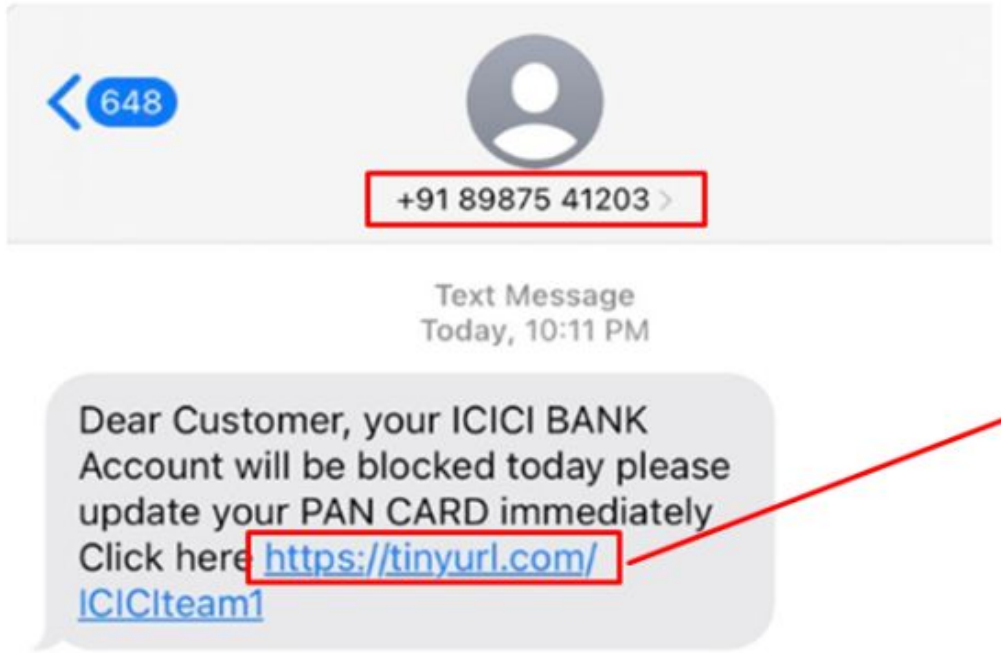


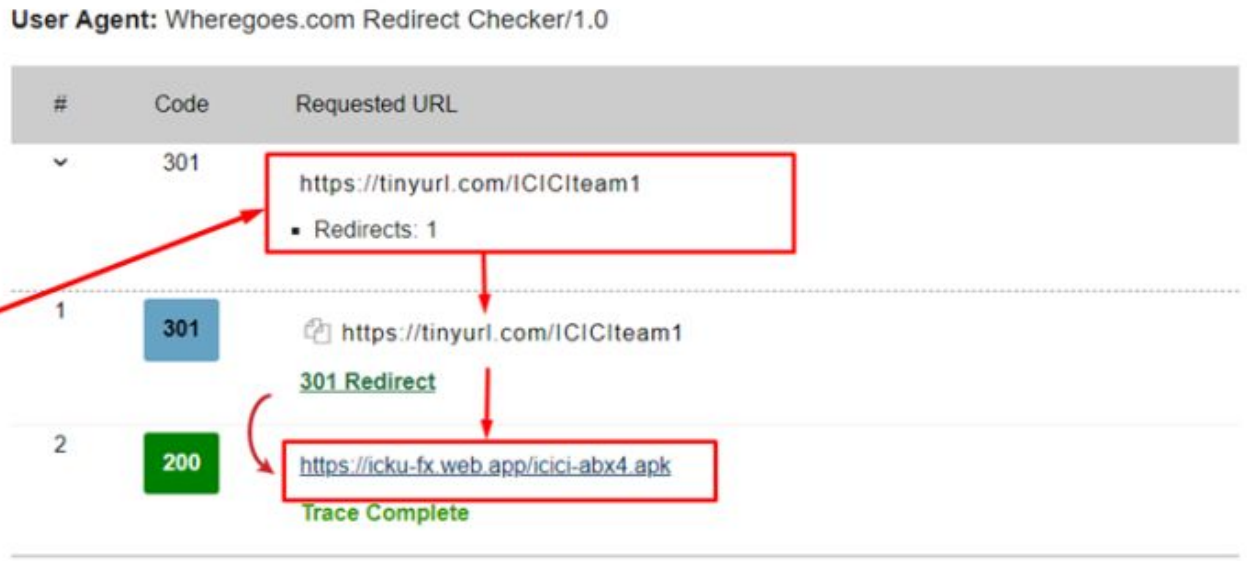


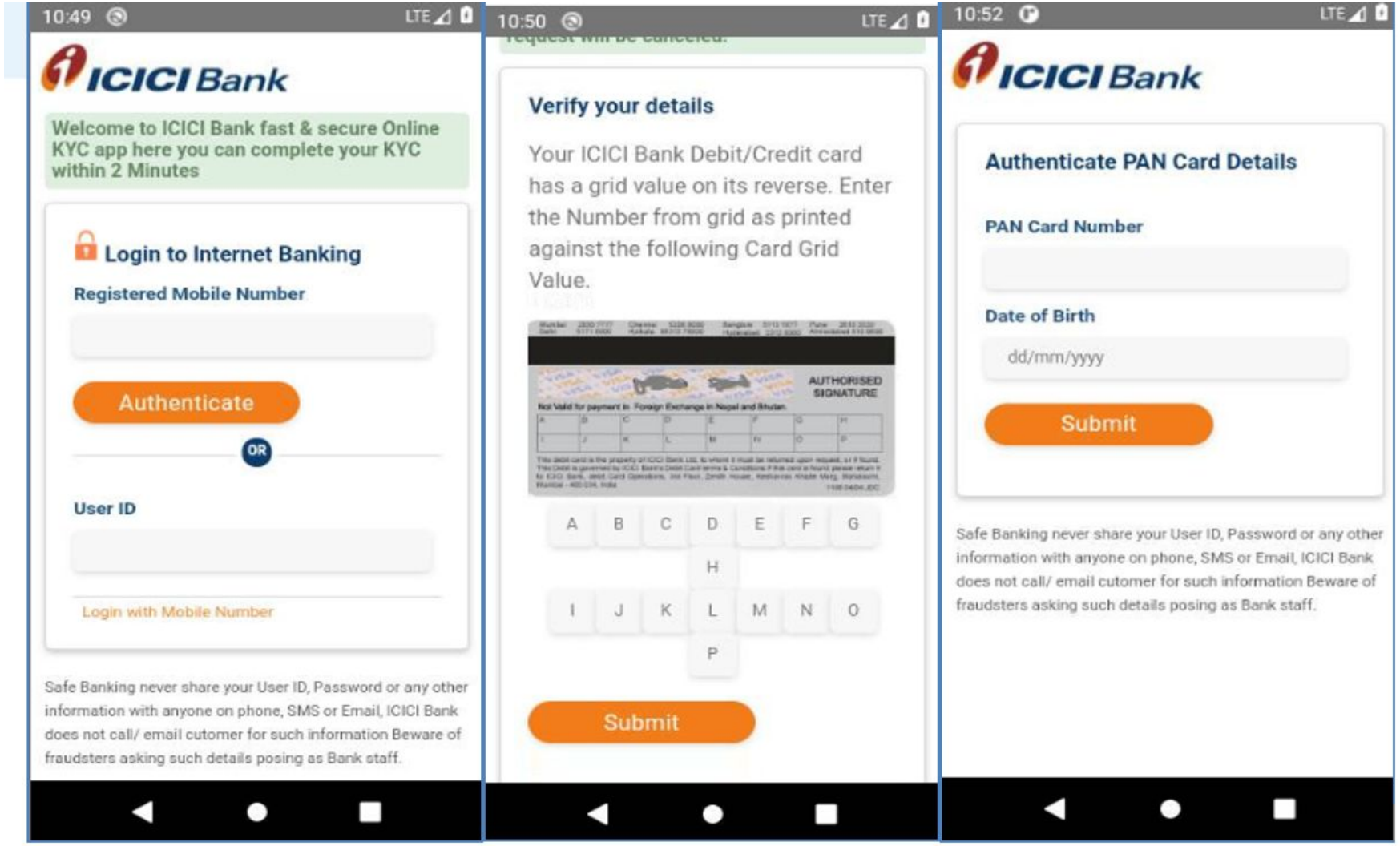




SMS Phishing link URL redirected to **Malicious APK**







The application is asking for the user's sensitive information like login credentials, credit/debit card grid value (printed on the card), PAN number, Date of Birth, etc.

Malicious Payload hosted on 'web.app' : https://icku-fx.web.app/icici-abx4.apk

Names

icici-abx4.apk

MD5	c2be5de66405d65b3fd23caec90b92cd
SHA-1	f631b05fe231f58ea8054d23c4023e9c48409616

Summary

Android Type	APK
Package Name	com.ikycappi.cxzx4
Main Activity	com.ikycapp.android.MainActivity
Internal Version	1
Displayed Version	1.0
Minimum SDK Version	22
Target SDK Version	32

Certificate Attributes

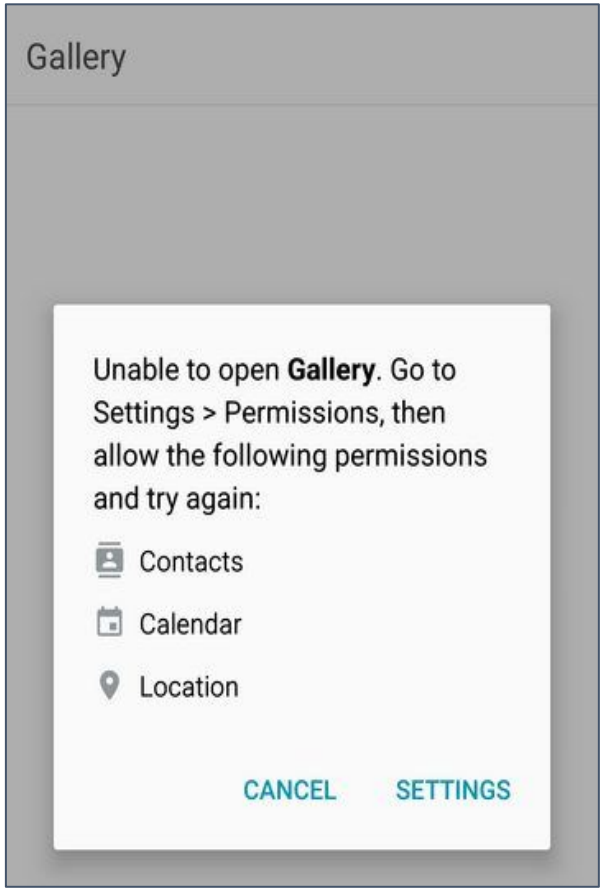
Valid From	2008-04-15 22:40:50
Valid To	2035-09-01 22:40:50
Serial Number	b3998086d056cffa
Thumbprint	27196e386b875e76adf700e7ea84e4c6eee33dfa

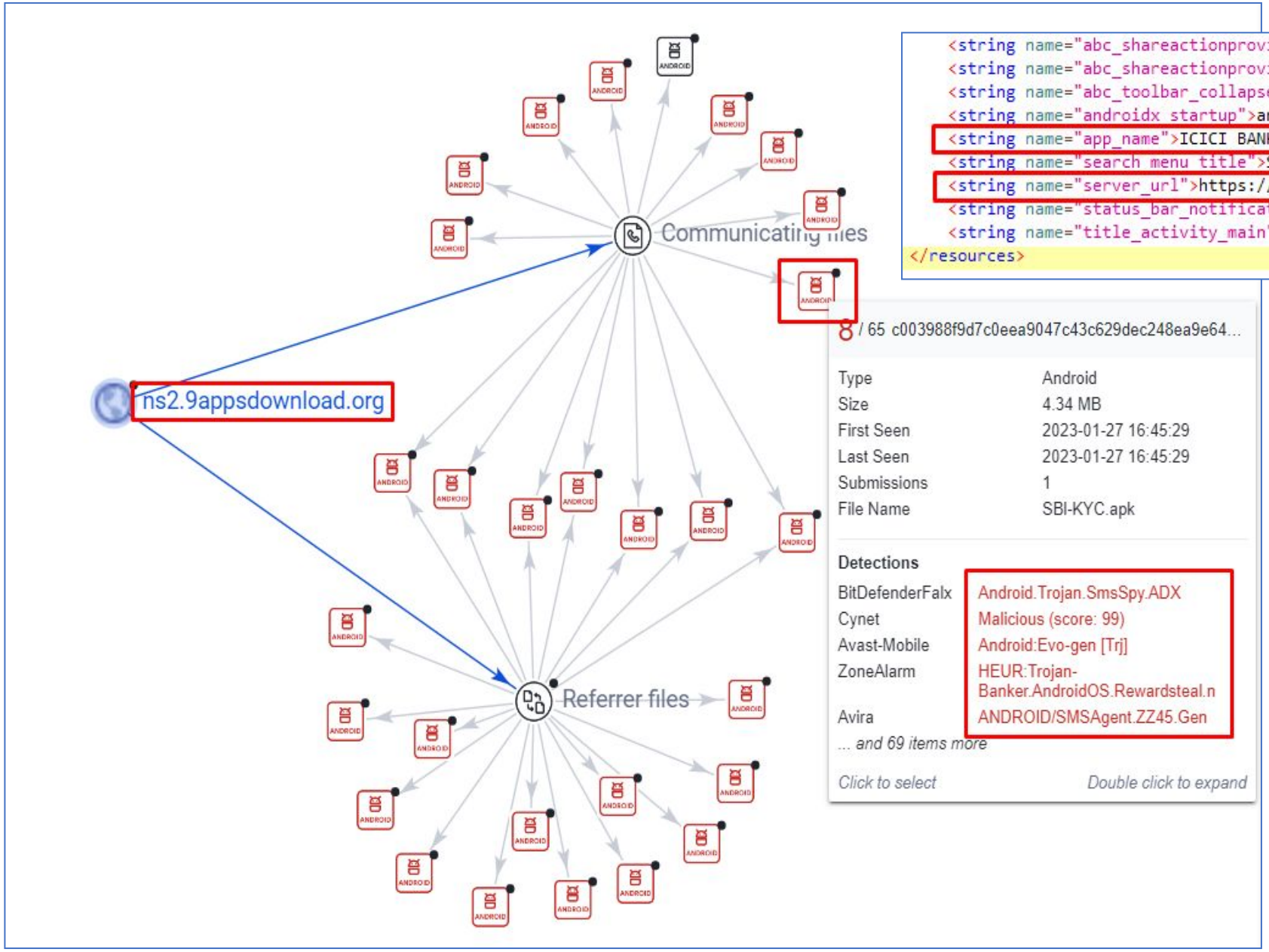
Certificate Subject

Distinguished Name	C:US, CN:Android, L:Mountain View, O:Android, ST:California, OU:Android, email:android@android.com
Email	android@android.com
Common Name	Android
Organization	Android
Organizational Unit	Android
Country Code	US
State	California
Locality	Mountain View

Permissions

- ⚠ android.permission.RECEIVE_SMS
- ⚠ android.permission.READ_SMS






```
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="androidx_startup">androidx.startup</string>
    <string name="app_name">ICICI BANK KYC</string>
    <string name="search_menu_title">Search</string>
    <string name="server_url">https://ns2.9appsdownload.org/app.php</string>
    <string name="status_bar_notification_info_overflow">999+</string>
    <string name="title_activity_main">ICICI BANK KYC</string>
</resources>
```

/ 65 c003988f9d7c0eea9047c43c629dec248ea9e64...

Type	Android
Size	4.34 MB
First Seen	2023-01-27 16:45:29
Last Seen	2023-01-27 16:45:29
Submissions	1
File Name	SBI-KYC.apk

Detections

BitDefenderFalx	Android.Trojan.SmsSpy.ADX
Cynet	Malicious (score: 99)
Avast-Mobile	Android:Evo-gen [Trj]
ZoneAlarm	HEUR:Trojan-Banker.AndroidOS.Rewardsteal.n
Avira	ANDROID/SMSAgent.ZZ45.Gen

... and 69 items more

Click to select *Double click to expand*

Hosting templates on phishing Server/Domains

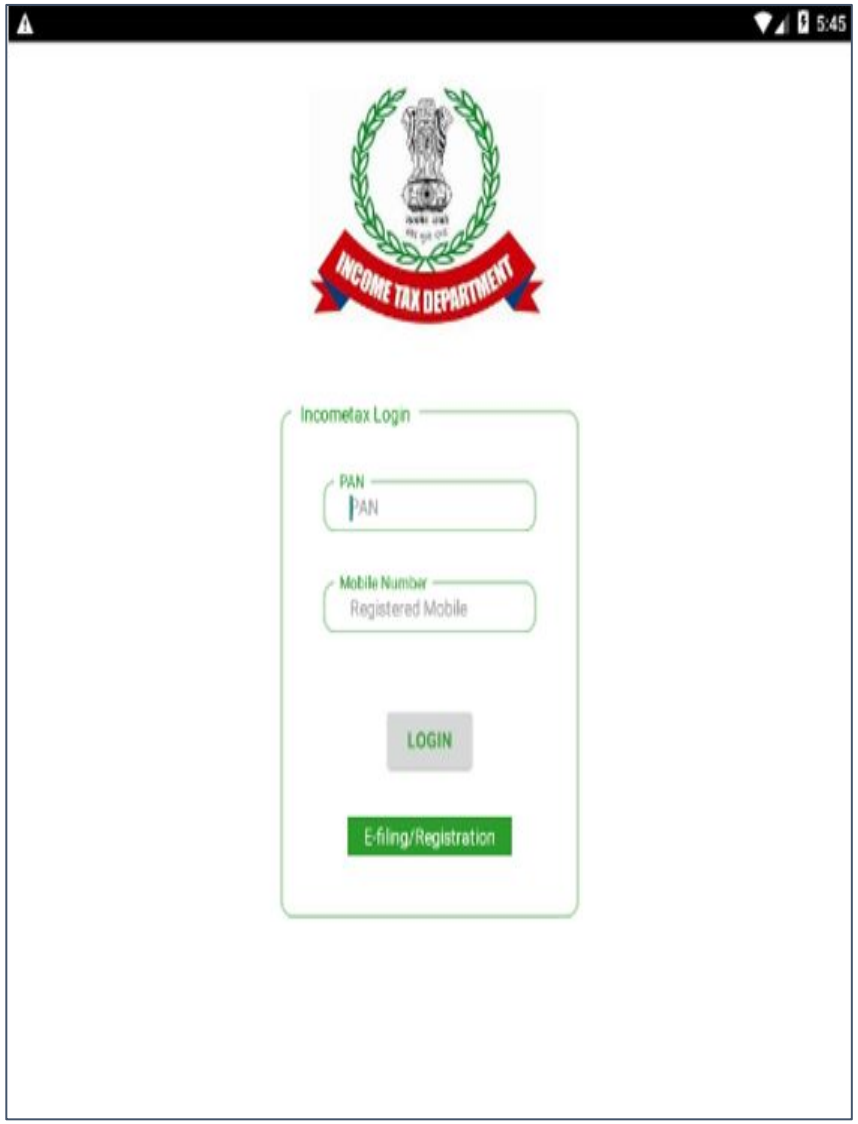
EXAMPLE 3

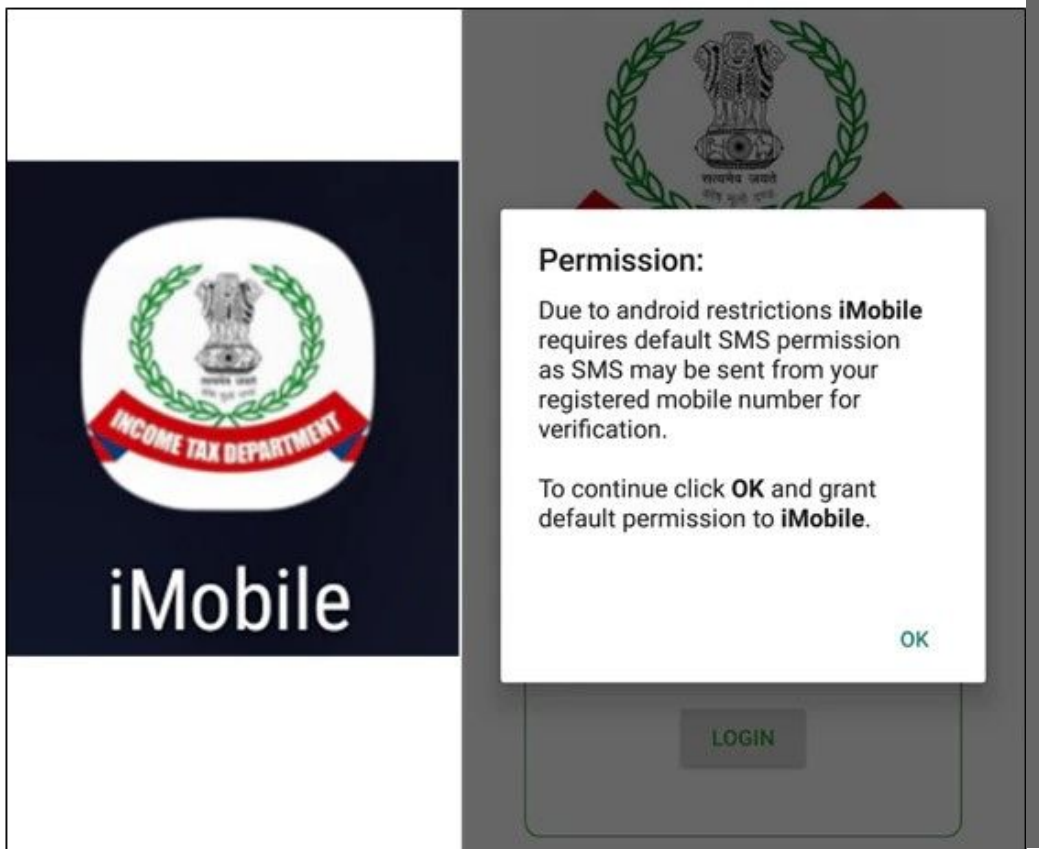
Example

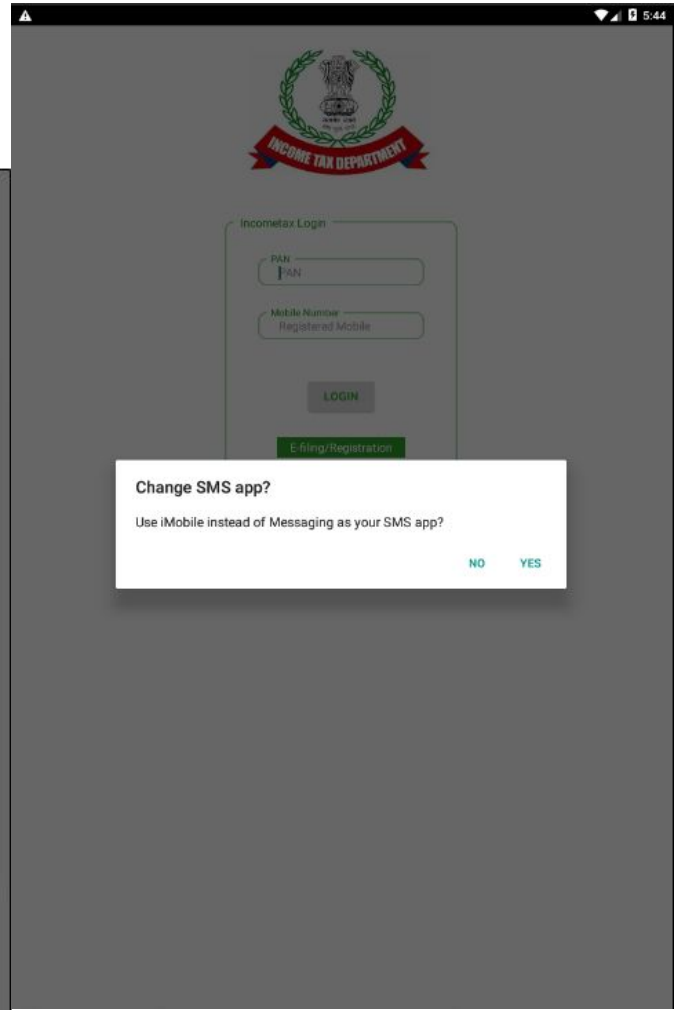

10:59
64%
WhatsApp
Update WhatsApp Messenger
WhatsApp Inc.
PEGI 3
INSTALL
Contains ads
1 MILLION
Downloads
4.2
6,614
Lifestyle
Similar
Update WhatsApp Messenger
READ MORE
Call your friends and family for free
Simple. Personal. Real time messaging.
Share your location or nearby places
10:59
64%
WhatsApp
WhatsApp Messenger
WhatsApp Inc.
PEGI 3
8.77 MB/18.40 MB
47%
Verified by Play Protect
You Might Also Like
MORE
Messenger Lite
FREE
4.4
Facebook Lite
FREE
4.2
YouTube
FREE
4.3
4.5
Similar Apps
MORE


WhatsApp Messenger
WhatsApp Inc. Communication
60,186,133
3+
This app is compatible with all of your devices.
Installed
WhatsApp Messenger
WhatsApp Inc.• Weather
271
3+
Loading device compatibility...
Add to Wishlist
Install
Whatsapp Messenger
WhatsApp .Inc ** Communication
484
16+
Contains ads
This app is compatible with all of your devices.
Add to Wishlist
Install

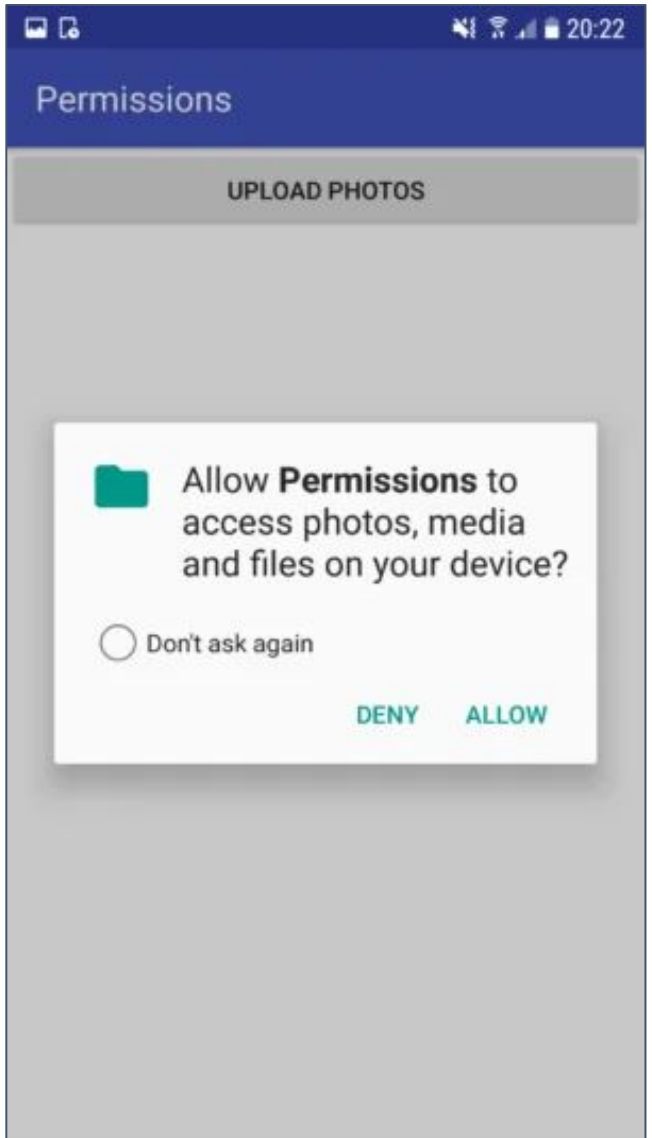
SMS PERMISSION

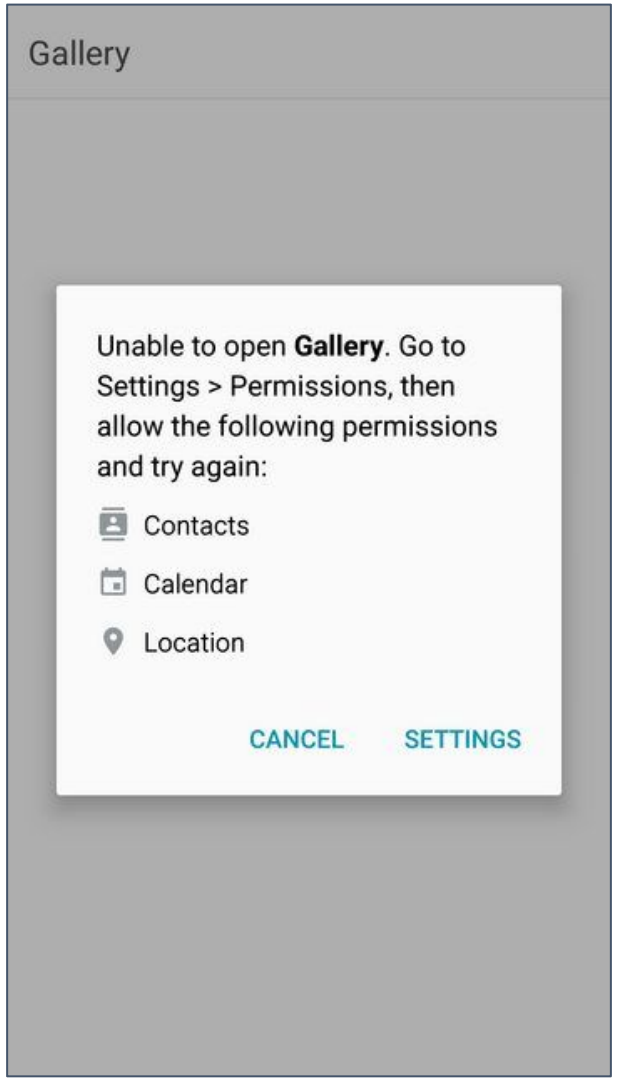


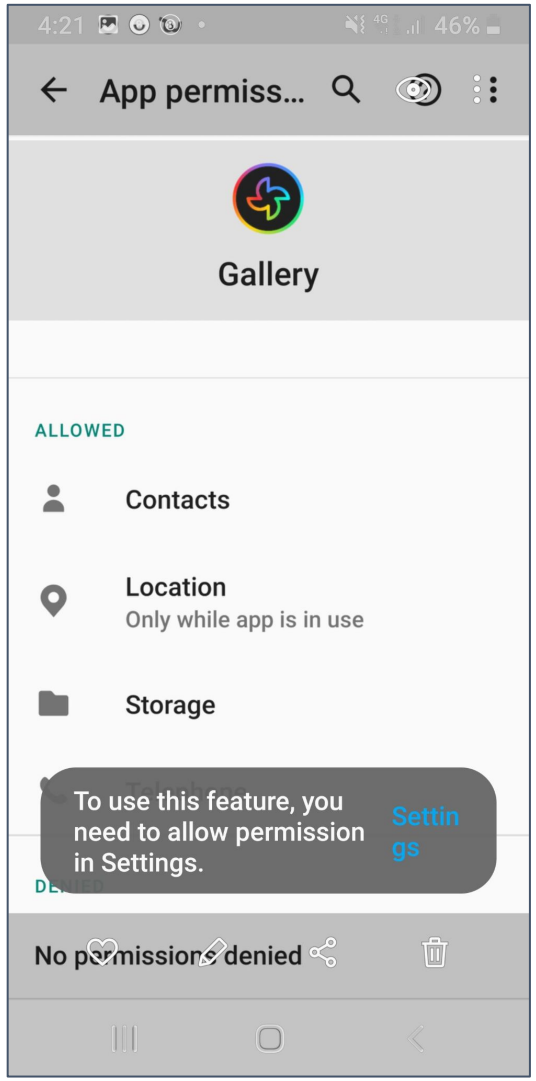




Permissions

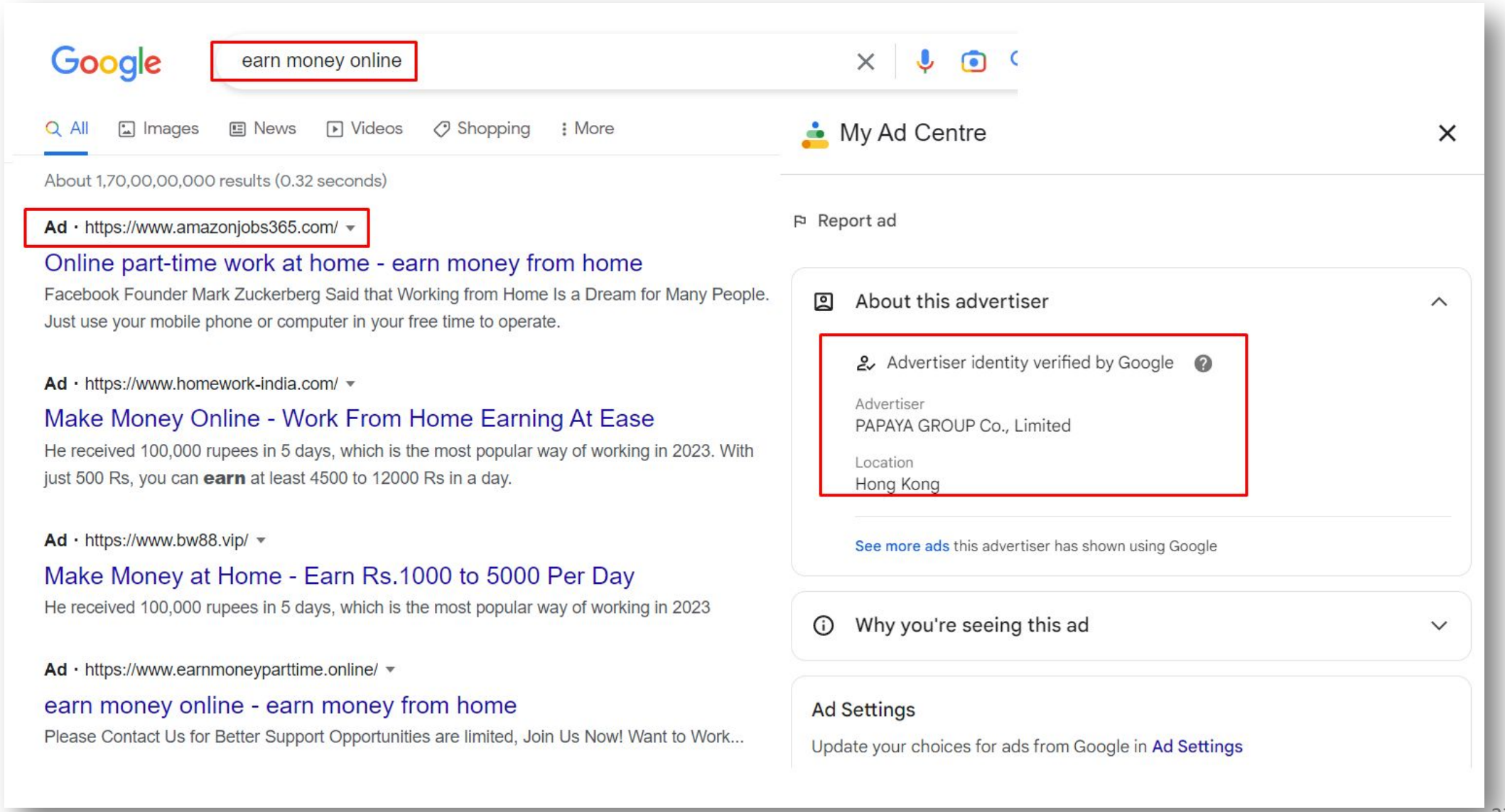






EXAMPLE 4

Search Engine



https://adstransparency.google.com/advertiser/AR02376743917019201537?region=IN&sig=AC0UAfwAAAAY_SStOYJNjGv1ZoM2GNP5w79Taw&hl=en_IN

PAPAYA GROUP Co., Limited

Any time | Shown in India | All formats

PAPAYA GROUP Co., Limited

Legal name: PAPAYA GROUP Co., Limited

Verified as based in Hong Kong

https://adstransparency.google.com/advertiser/AR02376743917019201537?region=IN&sig=AC0UAfwAAAAY_SStOYJNjGv1ZoM2GNP5w79Taw&hl=en_IN

Sponsored
gadgetslaboratory.com
www.gadgetslaboratory.com/
#1 Lightbulb Security Camera - 360° Front Door Security Cam
Best Light Bulb Security Cameras That Give You Perfect Peace of Mind & 24/7 Protection.

Phone Security, Virus Cleaner
Phone Cleaner
Google Play
Install

Tap Coin
Only for Malaysia
Google Play
Install

Balls Bricks Breaker 2
Casual arcade game.
Google Play
Install

Word Search Puzzle
Word Search 2021.
Google Play
Install

FTL VPN
The Best Free VPN Free Forever
Google Play
Install

Sponsored
www.piaproxy.com/
proxy pass ip address list
PIA proxy The best IP conversion software on the market, 200+ countries around the world

Ad · www.heyfriday.ai/
Ultimate AI Writer
Generate an article in 4-clicks: 500-word article in 5 minutes. Start Now.

Tap Coin
वर्ल्ड कप की 10 हाइलाइट्स
Google Play
इंस्टॉल

Sponsored
mobitracker.org
www.mobitracker.org/
Find Mobile Device Location - Just Need Phone Number
The best phone tracker 2022 - search phone number and get location, for all carriers

WeLive
obrolan video langsung
Google Play
Instal

Sponsored
News Break
www.newsbreak.com/
Savannah Local Newsletter
Stay up to date with what's happening in Savannah

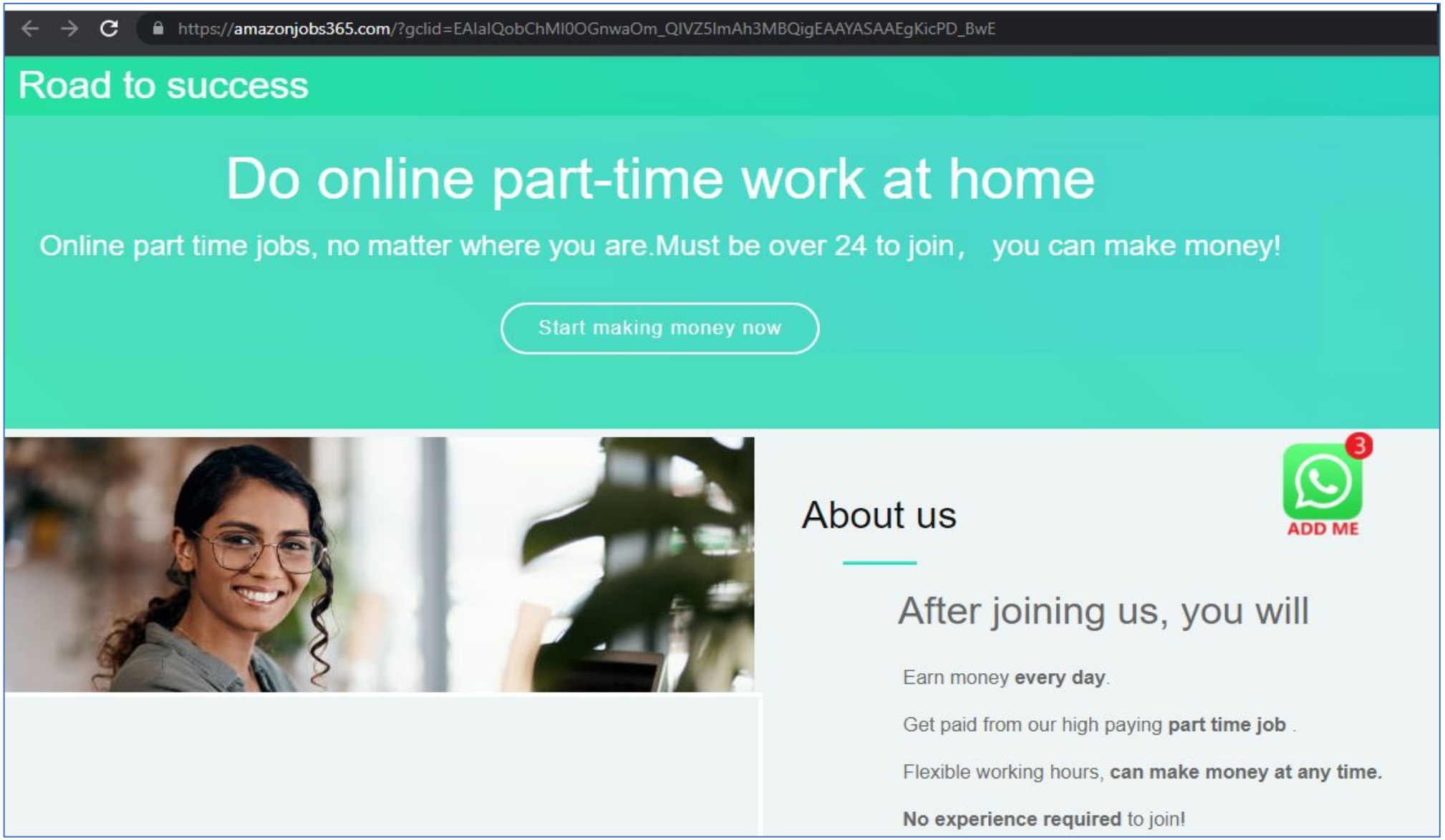
Sponsored
www.pyproxy.com/
Rotating Residential Proxies
High Quality Proxy Service, Unlimited Concurrent Sessions & Domains, As Low as $0.7/GB

Sponsored
my.octafx.com/
OctaFx Platform - OctaFx Sign up now
OctaFX Trading App is the official trading tool for both deposit and withdrawal. Join with Octafx. Free comission. Octafx is the best.

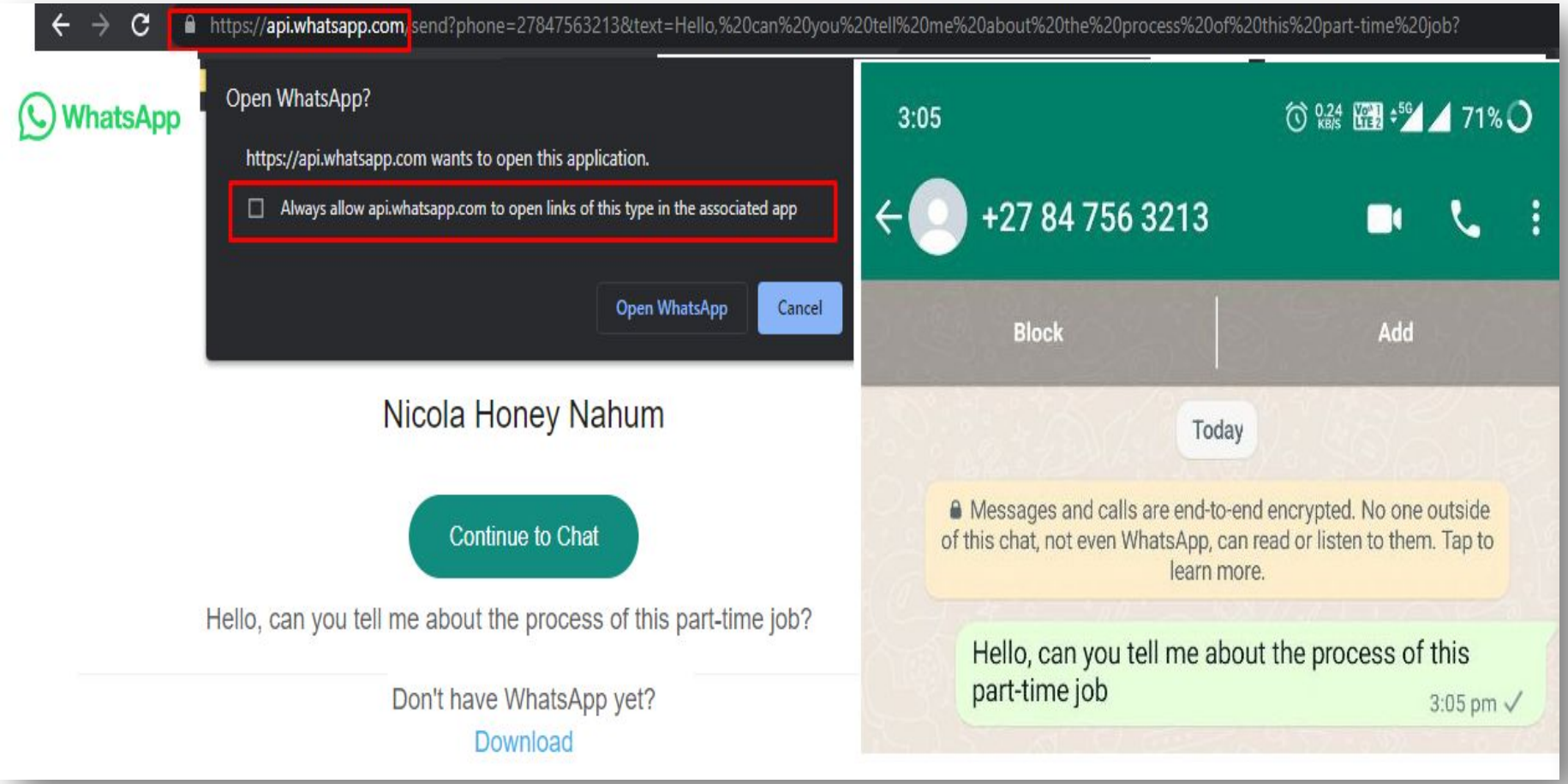
Deriv.com - DerIV - Deriv
Deriv
Deriv MT5
Sign up for a free demo
Contact Us

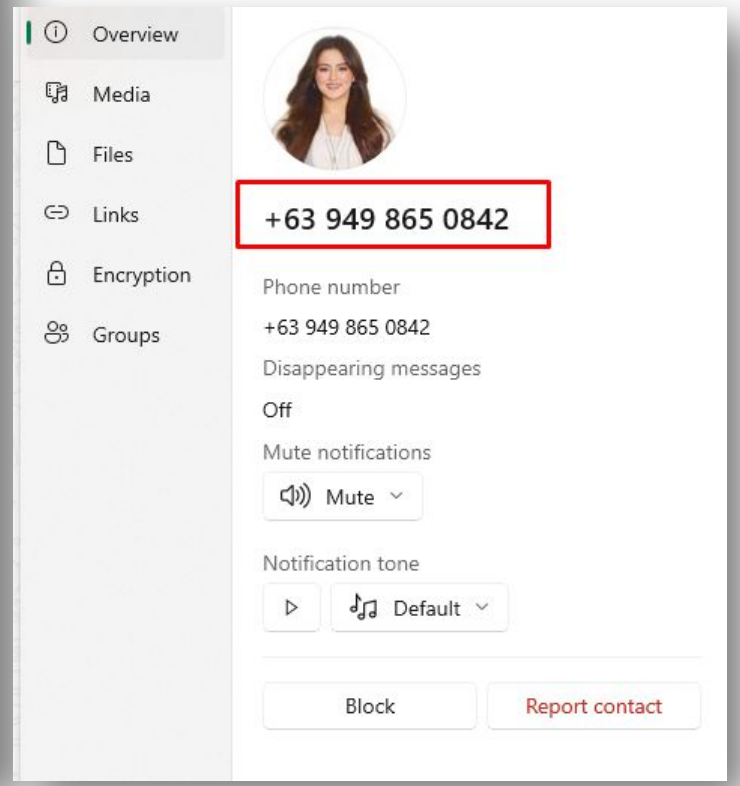
Tap Coin
इंग्लैंड बनाम ईरान
Google Play
इंस्टॉल

Redirection



Attack medium





Malware

people tend to trust text messages more than emails

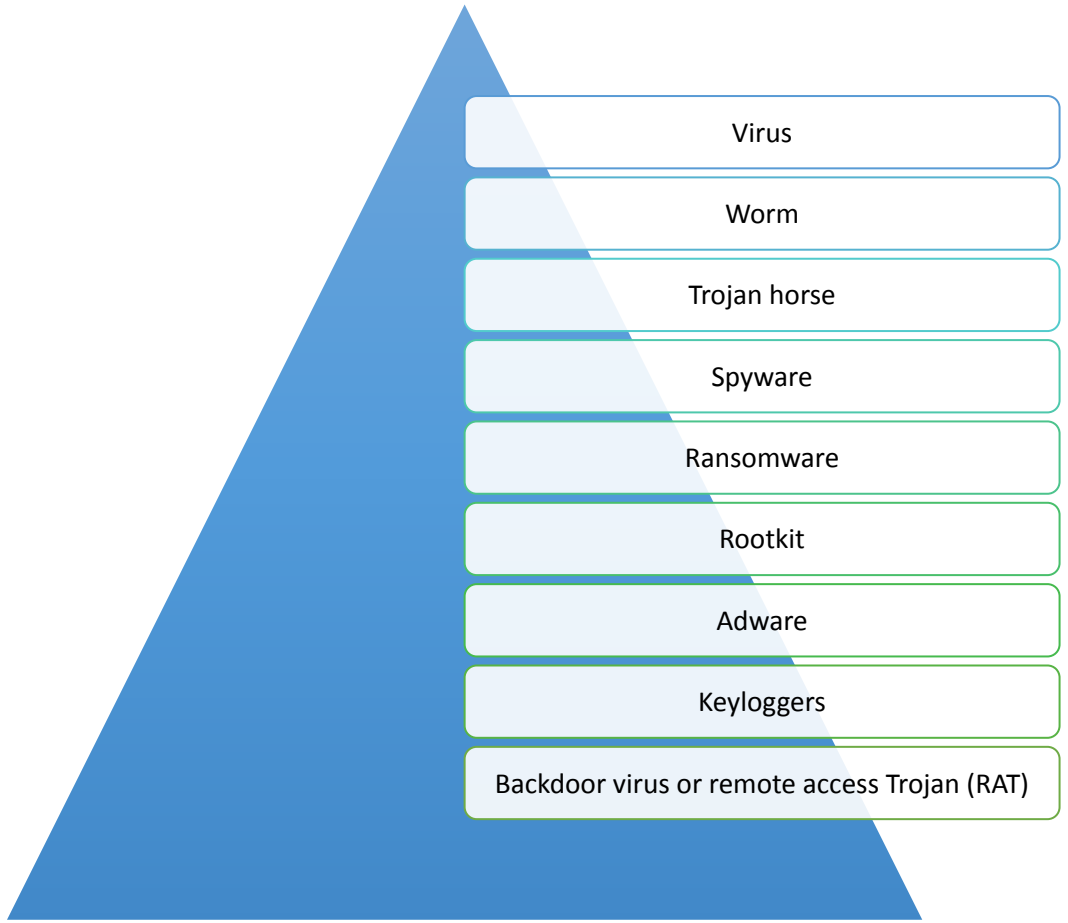
Malware is short for "malicious software"

cyber incidents. Also Push Pull agent facility through app

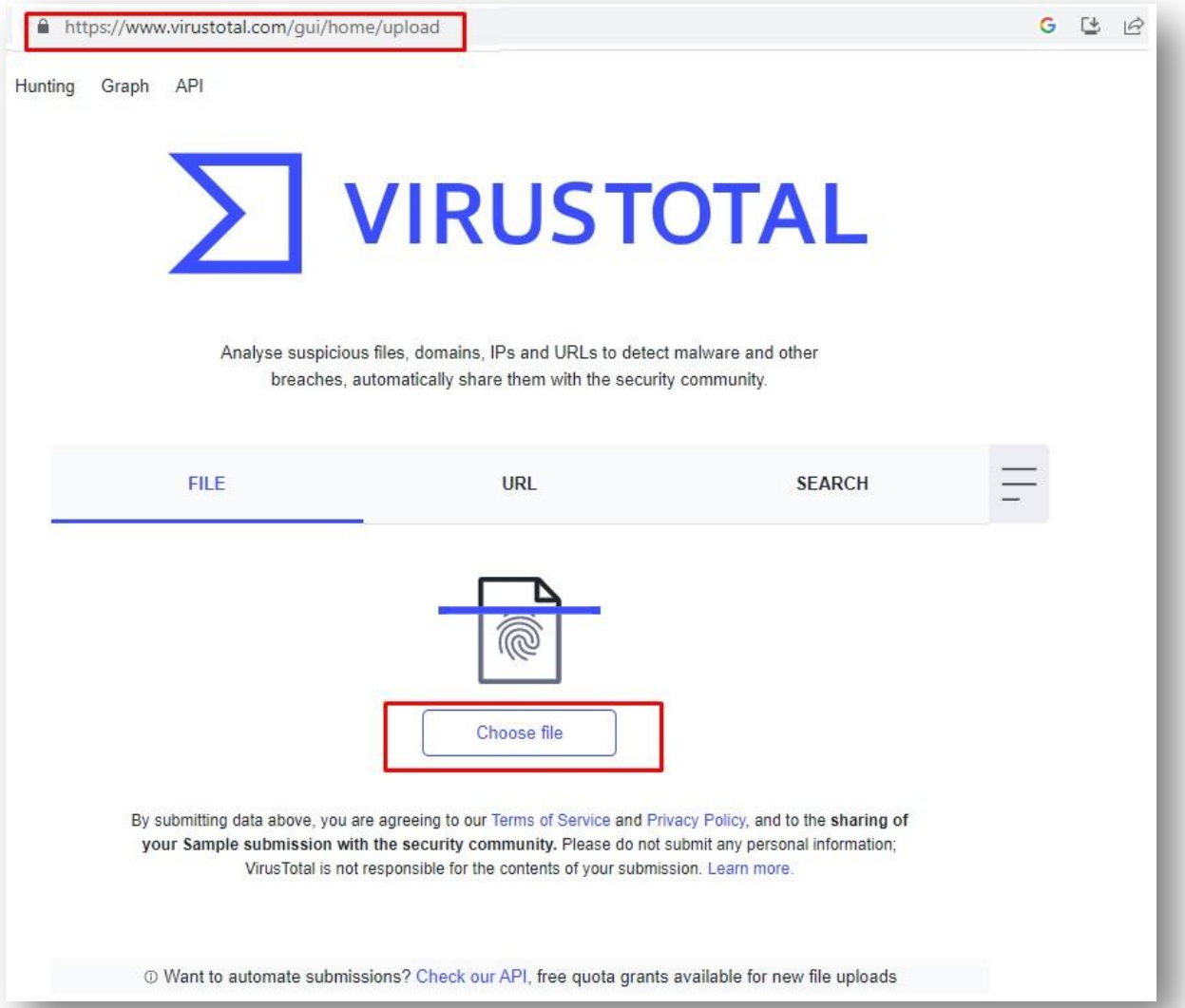
as call forwarding

services such as 'BOMBitUP', 'Blast', 'Bomber', etc

Some of the malwares are:

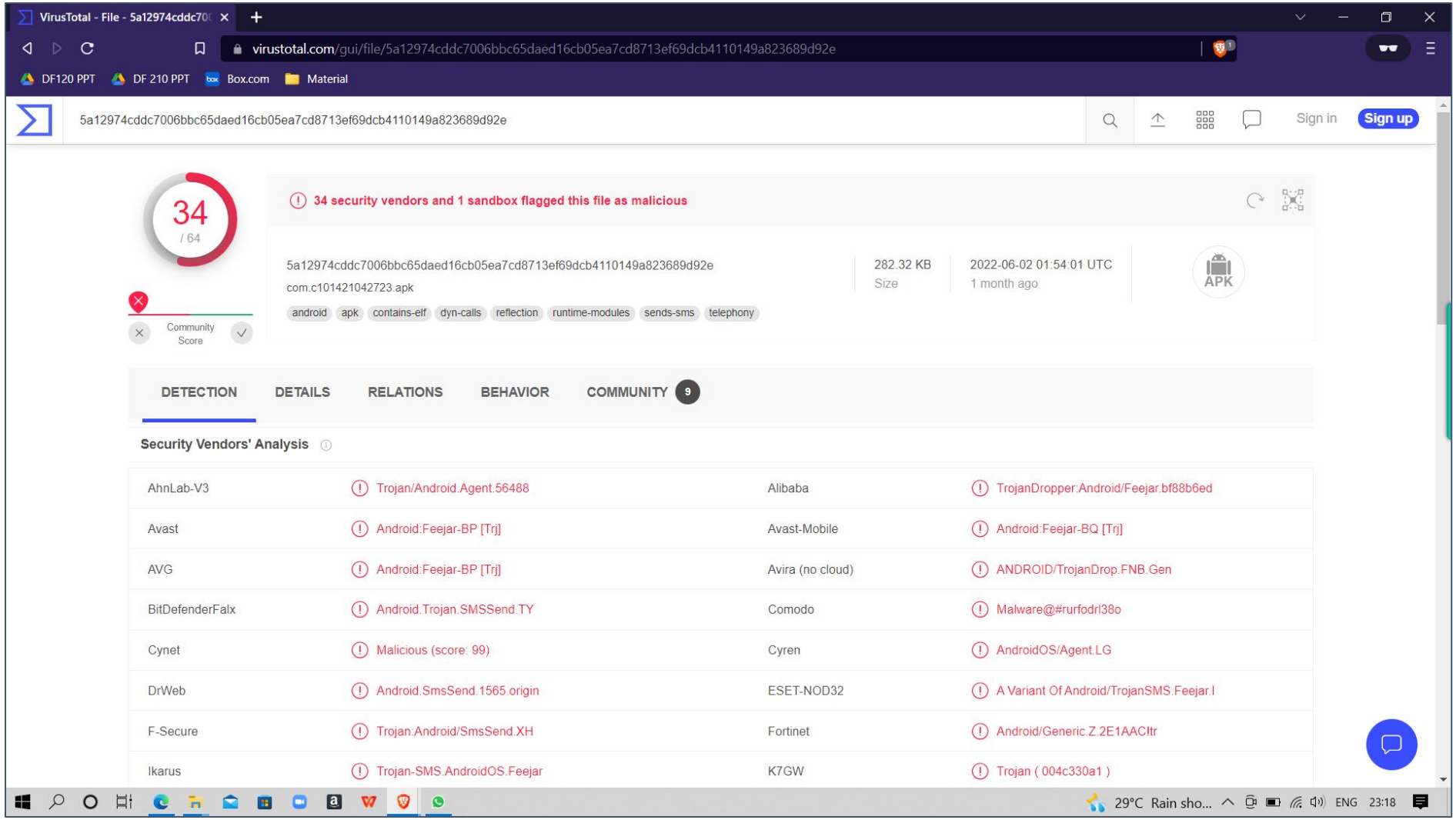


COUNTERMEASURE



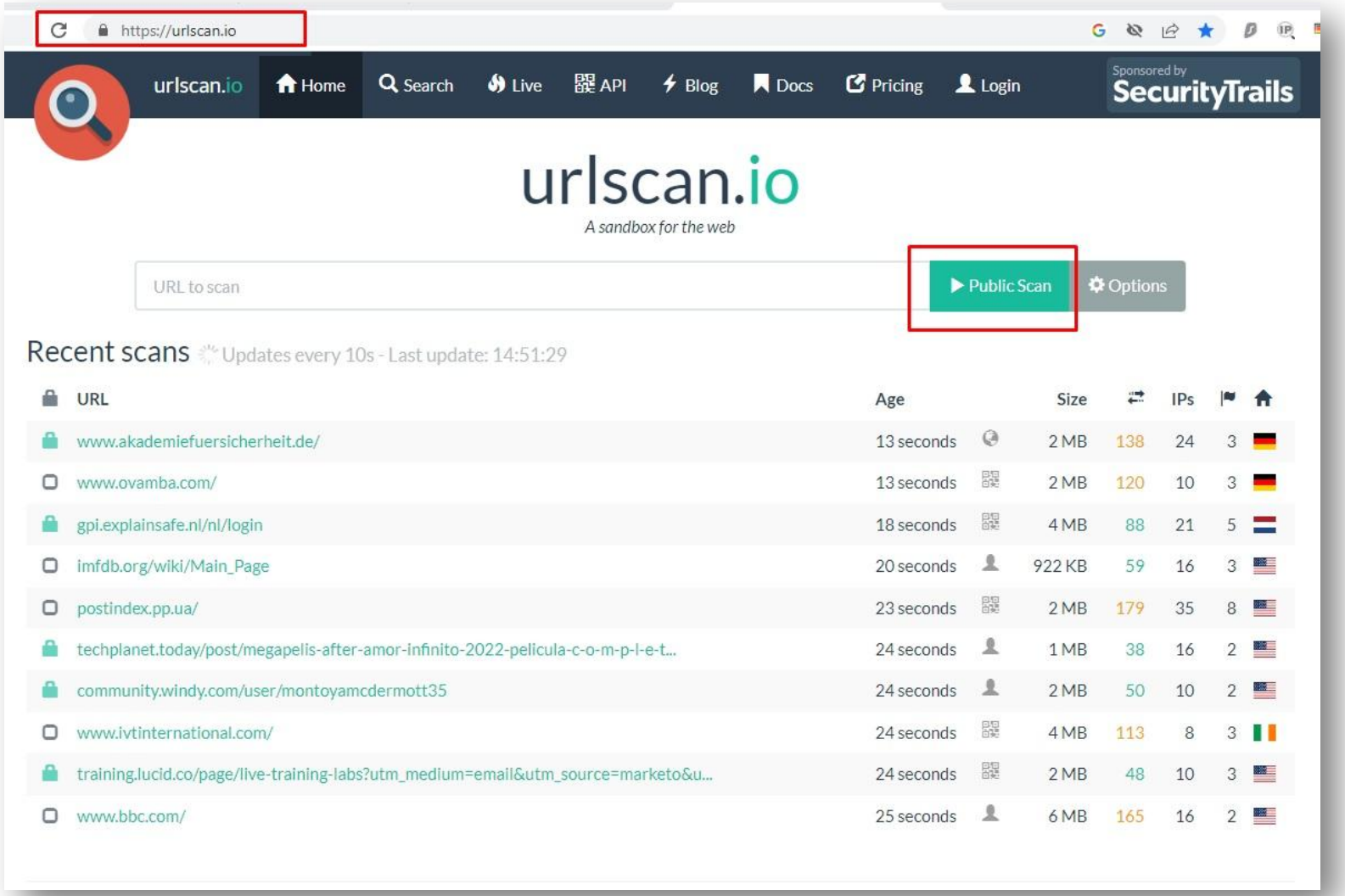
https://www.virustotal.com

COUNTERMEASURE

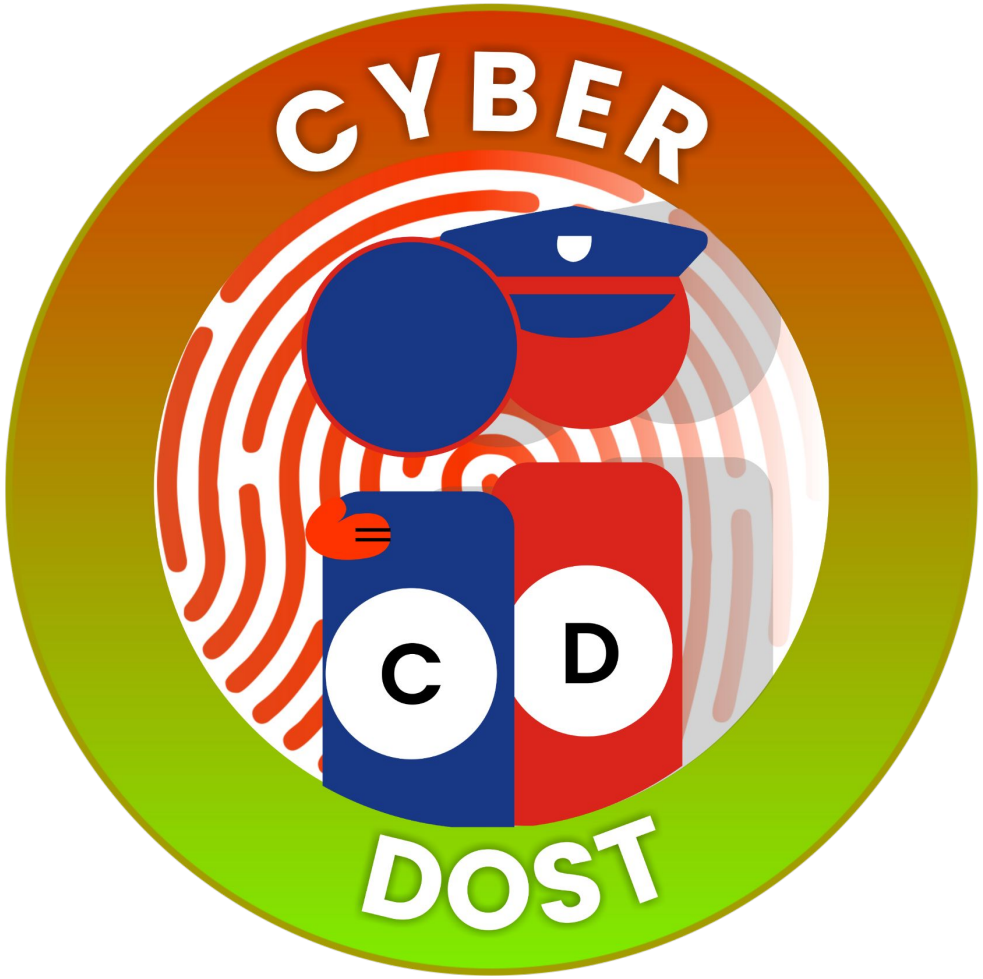


Virustotal will give the Output (Whether the APK is Malicious or Not)

COUNTERMEASURE



https://urlscan.io
/



Follow *CyberDost* on social media

- Get the latest Cyber Safety Tips
- Learn about various types of Scam Alerts
- Get updates on National and International Cyber news
- Learn about the achievements in the attempt to make the nation cyber safe
- Become a Cyber Volunteer and share the CyberDost content with your community
- Do your bit to stay vigilant and stay cyber safe!

@cyberdosti4c @CyberDosti4c @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c @cyberdost @cyberdost