vb 2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

MEGALO-(414E)-DON: UNCOVERING DATA ESPIONAGE, BLACKMAILING AND SHELL COMPANIES IN MOBILE LENDING APPS

Jagadeesh Chandraiah

Sophos, UK

jagadeesh.chandraiah@sophos.com

ABSTRACT

Years of pandemic, lockdowns, the cost-of-living crisis and rising inflation have taken money out of people's pockets, especially in developing nations, pushing an increasing number of people to rely on taking out personal loans. Traditional banks have been tightening their lending policies – borrowers need good credit scores, and in some countries they even ask for collateral to lend money in this tough economic climate. Spotting a gap in the market, several malevolent mobile lending applications have arisen to lend to individuals when they are in a vulnerable situation.

Mobile lending applications have been a problem on app platforms for years, with few legitimate apps and several fraudulent ones. Researchers have been finding lending applications that have been violating policies for years. App platforms have brought in several policy updates to curb illegal applications, but they circumvent these policies with fake information and have been thriving more than ever, particularly in the *Google Play* Store, due to *Android* having a higher market share in developing nations.

These lending apps claim to charge low interest and have longer repayment schedules, but in reality, have shorter repayment schedules ranging from seven days to a few weeks. Besides that, they collect vast amounts of personal data, identity details, device information, contacts, locations, SMS and call logs, and store these details in unknown third-party locations, violating various data regulations. Some countries even classify these as hostile. When victims fail to repay within a short duration, they start charging high interest and abuse their personal data by threatening to send sensitive data to friends/relatives on the contact list, post on social media and make threatening calls. Several people have lost lives through suicide, unable to bear the torture of the agents.

Technology-wise, there is a sophisticated infrastructure behind these apps, with professional-looking websites, the use of app frameworks, the use of packers to evade app platform policies, fake banking regulation certificates being created on websites to fool users, and user traffic being driven through social media and *Telegram* groups.

INTRODUCTION

The fintech revolution and emergence of digital apps should have helped new fintech businesses meet niche markets, and helped everyone from all spheres of life make financial decisions with transparent information, especially those that are less well served by traditional banks. In many developing countries, mobile is the only way of accessing the internet, and through the app platforms, users are able to access things they didn't have access to before, including lending apps.

According to a joint report by *Google* and *Apps Flyer* [1] there has been an increase in the installation of financial apps since the COVID-19 pandemic, and trends show an increase in searches for instant loan applications.

Having identified a gap in the market, several malevolent mobile lending applications have appeared, aiming to appeal to individuals when they are in a vulnerable situation and in need of a loan.

MOBILE LENDING APPS

There are several categories of mobile lending app, covering business loans, payday loans, shopping loans, credit card loans and automobile loans. But in this paper, we will only focus on personal loan (also known as instant loan) lending apps, particularly those targeting developing countries.

Google defines a personal loan [2] as: '... lending money from one individual, organization, or entity to an individual consumer on a nonrecurring basis, not for the purpose of financing purchase of a fixed asset or education.' And states that 'Personal loan consumers require information about the quality, features, fees, risks, and benefits of loan products in order to make informed decisions about whether to undertake the loan.'

Instant loan apps target vulnerable people in developing countries due to lax policies. Targeted countries include India, Nigeria, Kenya, Ghana, Thailand, Philippines, Indonesia, Vietnam, Pakistan, Sri Lanka, Bangladesh and Mexico.

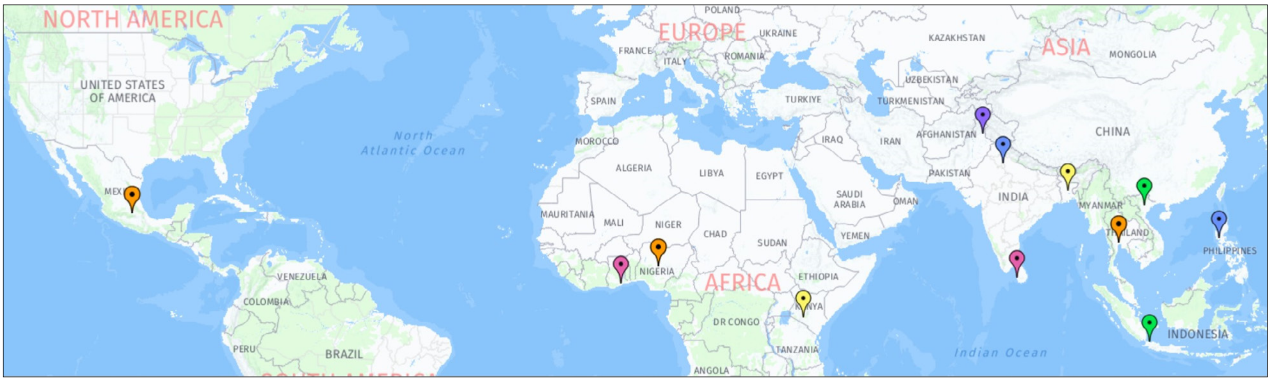


Figure 1: Major countries affected by personal loan apps.

The major lure of these data spyware applications is the possibility of having an instant loan with minimal documents. Traditional banks need several documents, collateral and can take weeks or months to provide loans [3]. Meanwhile, digital loan apps require fewer documents and disburse the loan in a matter of hours or days. Everything happens online without the need to go anywhere in person. This makes it an attractive option.

Process

Personal loan app applications involve several steps before the loan approval. Users are allowed to borrow on the amounts set in the app. These limits are usually small to medium, depending on the lender and borrower.

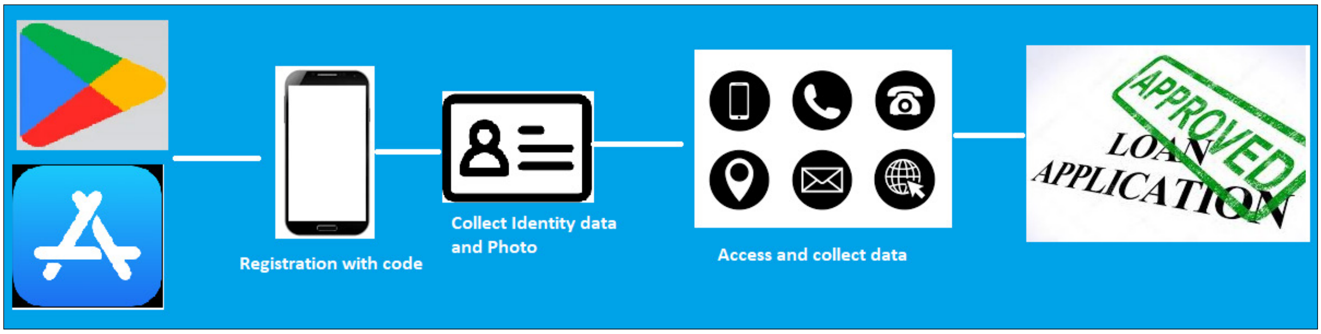
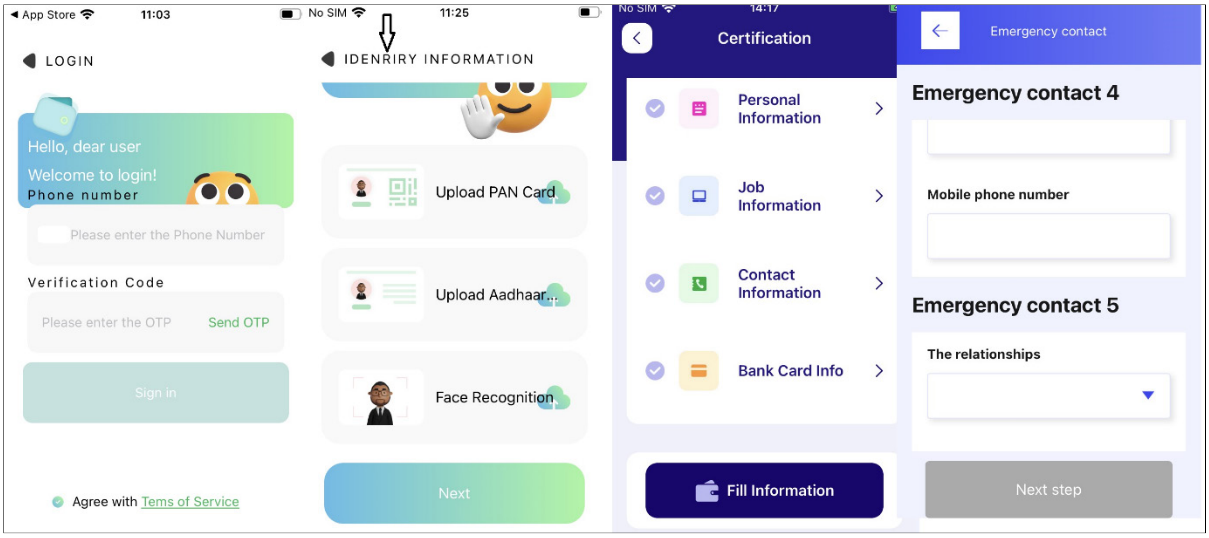


Figure 2: Loan application process.

- Step 1: Download the app from the *Apple App* Store or *Google Play* Store.
- Step 2: Enter mobile number, request verification or OTP code, and confirm.
- Step 3: Enter personal details such as name and address, upload identity information such as driving licence, national identity card, PAN card (social security number) and personal photo.
- Step 4: Contact details are collected.
- Step 5: Data is sent to a remote server for loan approval.

DATA COLLECTION AND PERMISSIONS

These applications collect vast amounts of data from their users. During the application process, they collect bank statements, identity documents, and the user's facial image.


App Store 11:03

LOGIN

Hello, dear user
Welcome to login!

Phone number
Please enter the Phone Number

Verification Code
Please enter the OTP Send OTP

Sign in

Agree with Terms of Service

No SIM 11:25

IDENRIRY INFORMATION

Upload PAN Card
Upload Aadhaar...
Face Recognition

Next

No SIM 14:17

Certification

Personal Information
Job Information
Contact Information
Bank Card Info

Fill Information

Emergency contact

Emergency contact 4
Mobile phone number

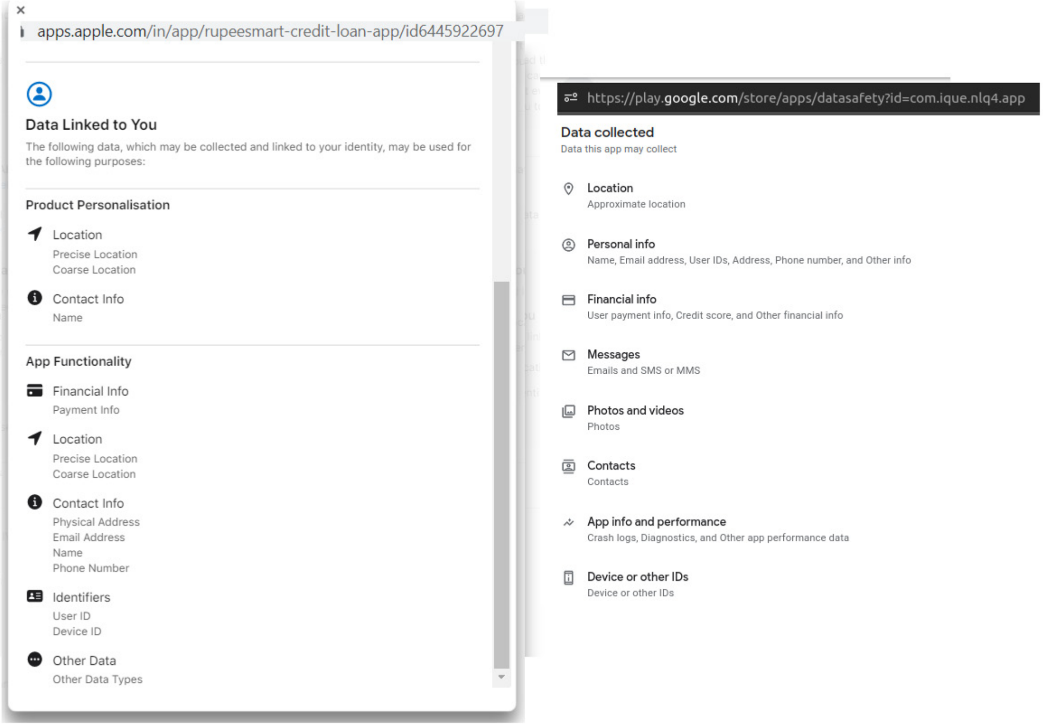
Emergency contact 5
The relationships

Next step

Figure 3: Screenshots of data collection in loan apps.

These apps will request permission for location, contacts, SMS messages, storage, Wi-Fi state, installed packages, telephone, camera, and calendar. Figures 4–6 show examples of permissions requested.

With this permission, they will be able to collect data about where the user resides, their list of friends, family, work colleagues and anyone else stored in the contacts list, the user's Wi-Fi details, SMS messages, pictures stored on the device, and other device information. Figure 7 outlines what the crooks claim is the purpose of collecting the information.



apps.apple.com/in/app/rupeesmart-credit-loan-app/id6445922697

Data Linked to You

The following data, which may be collected and linked to your identity, may be used for the following purposes:

Product Personalisation

- Location
  Precise Location
  Coarse Location
- Contact Info
  Name

App Functionality

- Financial Info
  Payment Info
- Location
  Precise Location
  Coarse Location
- Contact Info
  Physical Address
  Email Address
  Name
  Phone Number
- Identifiers
  User ID
  Device ID
- Other Data
  Other Data Types

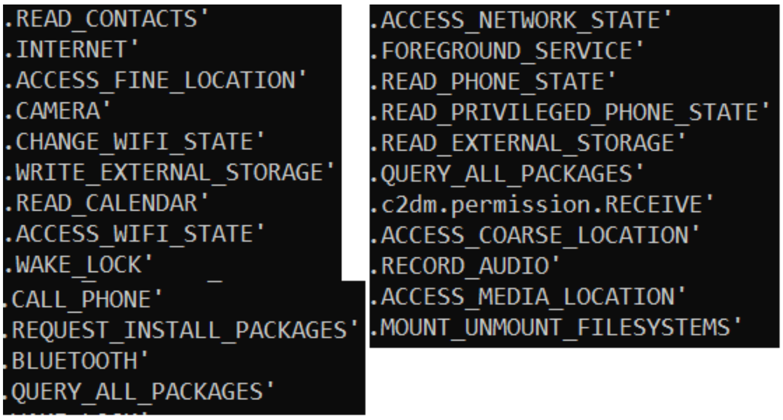
https://play.google.com/store/apps/datasafety?id=com.ique.nlq4.app

Data collected

Data this app may collect

- Location
  Approximate location
- Personal info
  Name, Email address, User IDs, Address, Phone number, and Other info
- Financial info
  User payment info, Credit score, and Other financial info
- Messages
  Emails and SMS or MMS
- Photos and videos
  Photos
- Contacts
  Contacts
- App info and performance
  Crash logs, Diagnostics, and Other app performance data
- Device or other IDs
  Device or other IDs

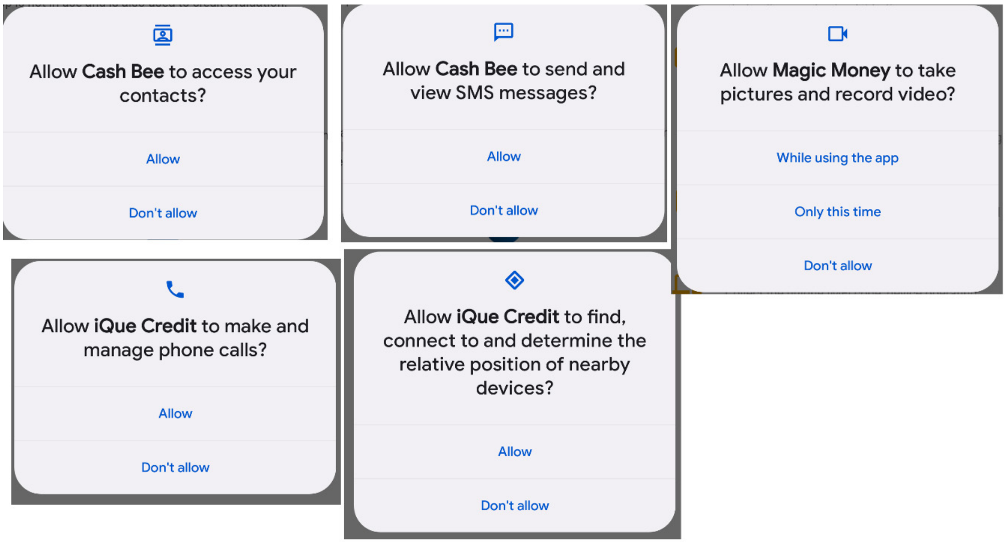
Figure 4: Data collected by one of the apps as displayed on App store and Play store page.



```
.READ_CONTACTS'
.INTERNET'
.ACCESS_FINE_LOCATION'
.CAMERA'
.CHANGE_WIFI_STATE'
.WRITE_EXTERNAL_STORAGE'
.READ_CALENDAR'
.ACCESS_WIFI_STATE'
.WAKE_LOCK'
.CALL_PHONE'
.REQUEST_INSTALL_PACKAGES'
.BLUETOOTH'
.QUERY_ALL_PACKAGES'
```

```
.ACCESS_NETWORK_STATE'
.FOREGROUND_SERVICE'
.READ_PHONE_STATE'
.READ_PRIVILEGED_PHONE_STATE'
.READ_EXTERNAL_STORAGE'
.QUERY_ALL_PACKAGES'
.c2dm.permission.RECEIVE'
.ACCESS_COARSE_LOCATION'
.RECORD_AUDIO'
.ACCESS_MEDIA_LOCATION'
.MOUNT_UNMOUNT_FILESYSTEMS'
```

Figure 5: Permissions requested by some of the apps.



Allow **Cash Bee** to access your contacts?

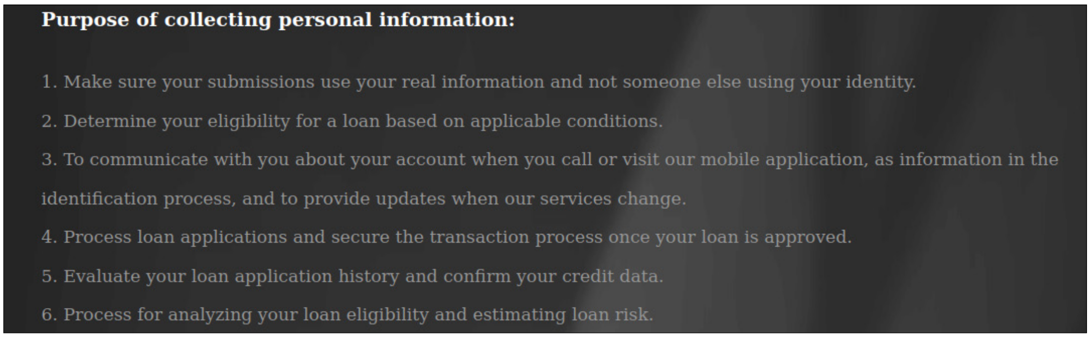
Allow **Cash Bee** to send and view SMS messages?

Allow **Magic Money** to take pictures and record video?

Allow **iQue Credit** to make and manage phone calls?

Allow **iQue Credit** to find, connect to and determine the relative position of nearby devices?

Figure 6: Permissions requested by some of the applications.



Purpose of collecting personal information:

1. Make sure your submissions use your real information and not someone else using your identity.
2. Determine your eligibility for a loan based on applicable conditions.
3. To communicate with you about your account when you call or visit our mobile application, as information in the identification process, and to provide updates when our services change.
4. Process loan applications and secure the transaction process once your loan is approved.
5. Evaluate your loan application history and confirm your credit data.
6. Process for analyzing your loan eligibility and estimating loan risk.

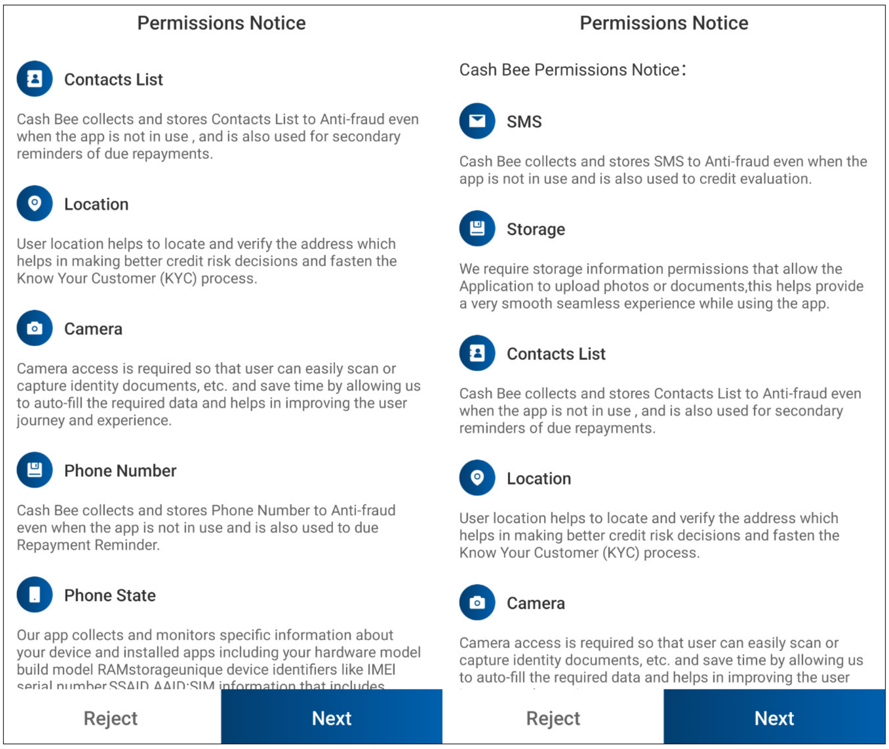
Figure 7: What crooks claim is the purpose of collecting information.

PRIVACY POLICY

Most of these apps have a privacy policy page that lists the data they'll collect. It discloses the information that will be collected, but does not mention that the data will be used for harassing and threatening purposes. Many of these apps also store, process and distribute data on unknown servers outside the country from which the data is collected without the consent of the users. Users granting these permissions are unaware that these permissions are abused for harassment reasons, as mentioned in the findings of [3].

Information they say will be collected by these apps includes:

- Personal information – name, email ID, date of birth
- Finance information – bank account number, income and debts
- Job information – employer, employer's contact details, job type and name
- Contacts list
- List of installed applications
- File directory information
- SMS information – SMS content, title
- Device information – OS type, screen resolution, IP address, manufacturer & model
- Images and videos
- Location – precise location of the user



Permissions Notice

Contacts List

Cash Bee collects and stores Contacts List to Anti-fraud even when the app is not in use , and is also used for secondary reminders of due repayments.

Location

User location helps to locate and verify the address which helps in making better credit risk decisions and fasten the Know Your Customer (KYC) process.

Camera

Camera access is required so that user can easily scan or capture identity documents, etc. and save time by allowing us to auto-fill the required data and helps in improving the user journey and experience.

Phone Number

Cash Bee collects and stores Phone Number to Anti-fraud even when the app is not in use and is also used to due Repayment Reminder.

Phone State

Our app collects and monitors specific information about your device and installed apps including your hardware model build model RAMstorageunique device identifiers like IMEI serial number SSAID AAID:SIM information that includes

Permissions Notice

Cash Bee Permissions Notice:

SMS

Cash Bee collects and stores SMS to Anti-fraud even when the app is not in use and is also used to credit evaluation.

Storage

We require storage information permissions that allow the Application to upload photos or documents,this helps provide a very smooth seamless experience while using the app.

Contacts List

Cash Bee collects and stores Contacts List to Anti-fraud even when the app is not in use , and is also used for secondary reminders of due repayments.

Location

User location helps to locate and verify the address which helps in making better credit risk decisions and fasten the Know Your Customer (KYC) process.

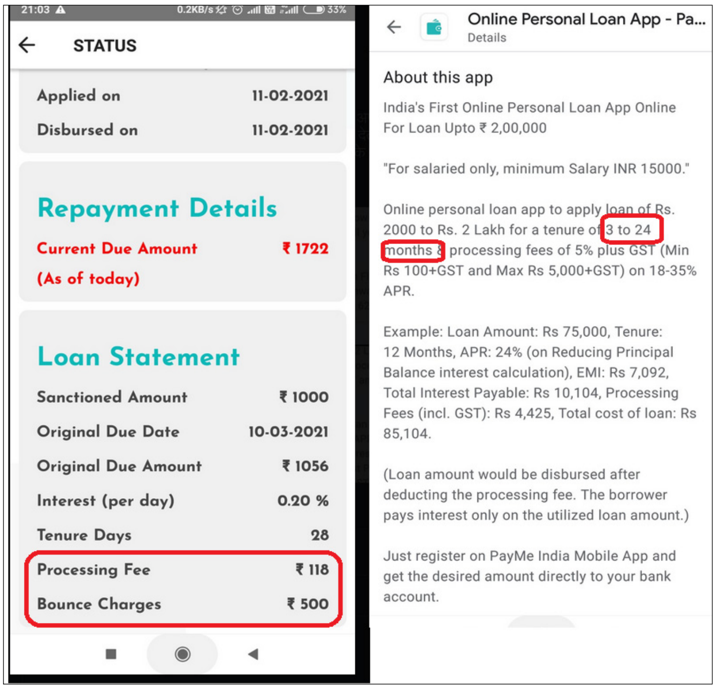
Camera

Camera access is required so that user can easily scan or capture identity documents, etc. and save time by allowing us to auto-fill the required data and helps in improving the user

Figure 8: Privacy policy page.

PROCESSING FEE AND SHORT TENURE

These apps charge extremely high interest rates, processing fees, and fake taxes to deduct lots of money from the source. At the peak of these app operations during 2019 and 2020, some of them charged between 200% and 300% annualized interest rates [4], as well as processing fees and tax. Later, the interest rates came down but were still high compared to legitimate banks. Deceitful charges are still a common feature; after fees and initial interest, 30–50% is still deducted from the principal.



STATUS

Applied on	11-02-2021
Disbursed on	11-02-2021

Repayment Details

Current Due Amount (As of today)	₹ 1722

Loan Statement

Sanctioned Amount	₹ 1000
Original Due Date	10-03-2021
Original Due Amount	₹ 1056
Interest (per day)	0.20 %
Tenure Days	28
Processing Fee	₹ 118
Bounce Charges	₹ 500

Online Personal Loan App - Pa...
Details

About this app

India's First Online Personal Loan App Online For Loan Upto ₹ 2,00,000

"For salaried only, minimum Salary INR 15000."

Online personal loan app to apply loan of Rs. 2000 to Rs. 2 Lakh for a tenure of 3 to 24 months & processing fees of 5% plus GST (Min Rs 100+GST and Max Rs 5,000+GST) on 18-35% APR.

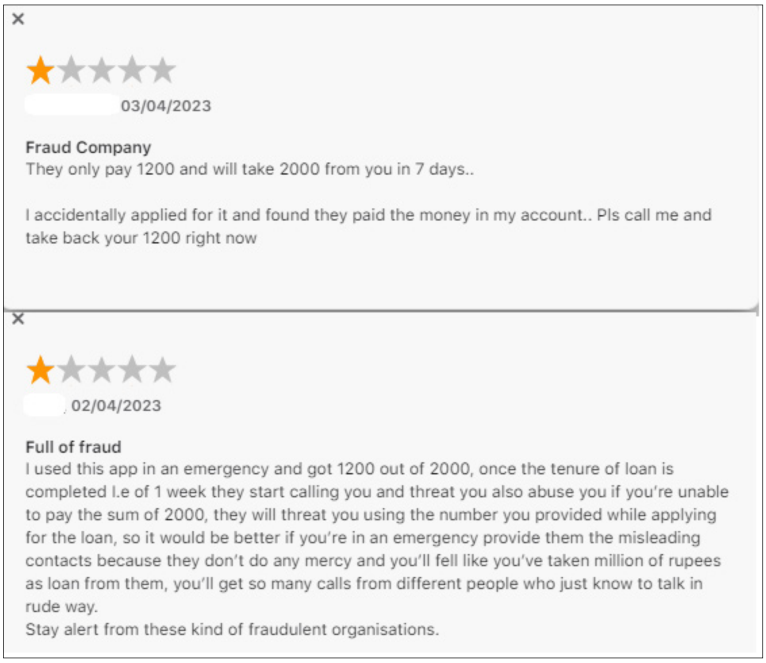
Example: Loan Amount: Rs 75,000, Tenure: 12 Months, APR: 24% (on Reducing Principal Balance interest calculation), EMI: Rs 7,092, Total Interest Payable: Rs 10,104, Processing Fees (incl. GST): Rs 4,425, Total cost of loan: Rs 85,104.

(Loan amount would be disbursed after deducting the processing fee. The borrower pays interest only on the utilized loan amount.)

Just register on PayMe India Mobile App and get the desired amount directly to your bank account.

Figure 9: More than 50% charges and less than one month tenure as opposed to three to 24 months as advertised on the app platform.

When you read through the reviews for some of the apps in the *App Store*, you'll notice many users complaining about getting only 60% of the borrowed amount. Borrowers using these apps end up repaying principal, which wasn't even near enough to what was advertised.



★☆☆☆☆
03/04/2023

Fraud Company
They only pay 1200 and will take 2000 from you in 7 days..

I accidentally applied for it and found they paid the money in my account.. Pls call me and take back your 1200 right now

★☆☆☆☆
02/04/2023

Full of fraud
I used this app in an emergency and got 1200 out of 2000, once the tenure of loan is completed I.e of 1 week they start calling you and threat you also abuse you if you're unable to pay the sum of 2000, they will threat you using the number you provided while applying for the loan, so it would be better if you're in an emergency provide them the misleading contacts because they don't do any mercy and you'll fell like you've taken million of rupees as loan from them, you'll get so many calls from different people who just know to talk in rude way.
Stay alert from these kind of fraudulent organisations.

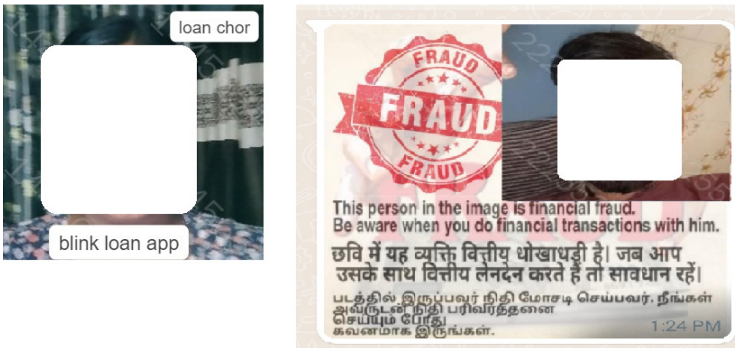
Figure 10: App store user reviews showing high processing fee.

Another way they make money is by advertising a long loan term, typically 60–90 days or more, but instead asking for repayment within a week in many instances and a couple of weeks at the latest.

BLACKMAIL AND SUICIDES

The loan apps gather data from the devices they are installed on and use that information to threaten users. They manipulate images collected from the device (as shown in Figure 11), often trying to make them look obscene, before sending them to the user's contact list. In some instances, if the borrower is female and they are unable to return the loan, they have been asked to send nude videos [5].

As shown in Figure 12, the crooks threaten the borrower that they will make nude media for distribution.

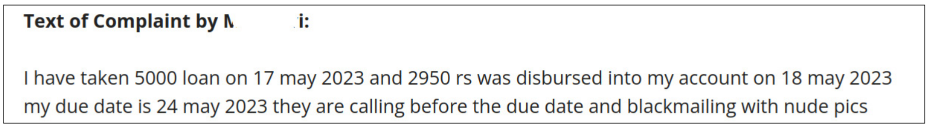


This person in the image is financial fraud.
Be aware when you do financial transactions with him.

छवि में यह व्यक्ति वित्तीय धोखाधड़ी है। जब आप
उसके साथ वित्तीय लेनदेन करते हैं तो सावधान रहें।

படத்தில் இருப்பவர் நிதி மோசடி செய்பவர். நீங்கள்
அவருடன் நிதி பரிவர்த்தனை
செய்யும் போது
கவனமாக இருங்கள்.

Figure 11: Manipulated images sent out to contact list phone numbers.



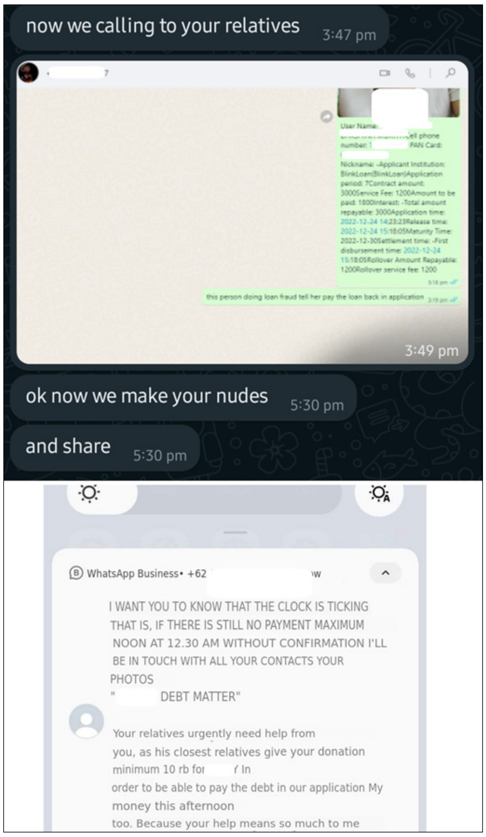
Text of Complaint by N[redacted]i:

I have taken 5000 loan on 17 may 2023 and 2950 rs was disbursed into my account on 18 may 2023 my due date is 24 may 2023 they are calling before the due date and blackmailing with nude pics

Figure 12: Court complaint screenshot from a borrower from India.

Clearly, should there be are any sensitive videos in the gallery on the device, it will be a great worry for the borrower as they do not know what else will be done besides sending them to those on their contact list.

Most of these apps are illegal, yet when sending out messages, they threaten to prosecute borrowers according to the law if they are late or unable to repay. Tragically, under the pressure of these extreme (and false) threats, and unable to face the shame that is inflicted on them, some vulnerable people have taken their own lives [6, 7].



now we calling to your relatives 3:47 pm

User Name: [redacted] Cell phone number: [redacted] PAN Card: [redacted] Nickname: -Applicant Institution: BlinkLoan(BlinkLoan)Application period: 7Contract amount: 3000Service Fee: 1200Amount to be paid: 1800Interest: -Total amount repayable: 3000Application time: 2022-12-24 14:23:23Release time: 2022-12-24 15:18:05Maturity Time: 2022-12-30Settlement time: -First disbursement time: 2022-12-24 15:18:05Rollover Amount Repayable: 1200Rollover service fee: 1200 3:18 pm

this person doing loan fraud tell her pay the loan back in application 3:19 pm

3:49 pm

ok now we make your nudes 5:30 pm

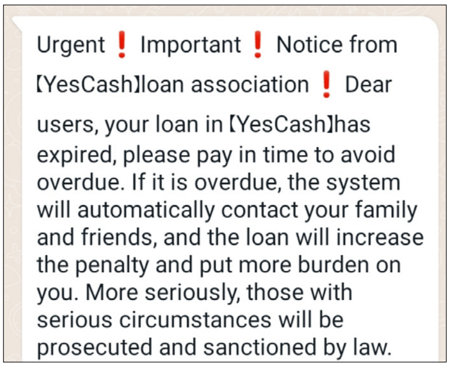
and share 5:30 pm

WhatsApp Business• +62 [redacted] w

I WANT YOU TO KNOW THAT THE CLOCK IS TICKING
THAT IS, IF THERE IS STILL NO PAYMENT MAXIMUM
NOON AT 12.30 AM WITHOUT CONFIRMATION I'LL
BE IN TOUCH WITH ALL YOUR CONTACTS YOUR
PHOTOS
"[redacted] DEBT MATTER"

Your relatives urgently need help from
you, as his closest relatives give your donation
minimum 10 rb for [redacted] In
order to be able to pay the debt in our application My
money this afternoon
too. Because your help means so much to me

Figure 13: Threatening WhatsApp messages.



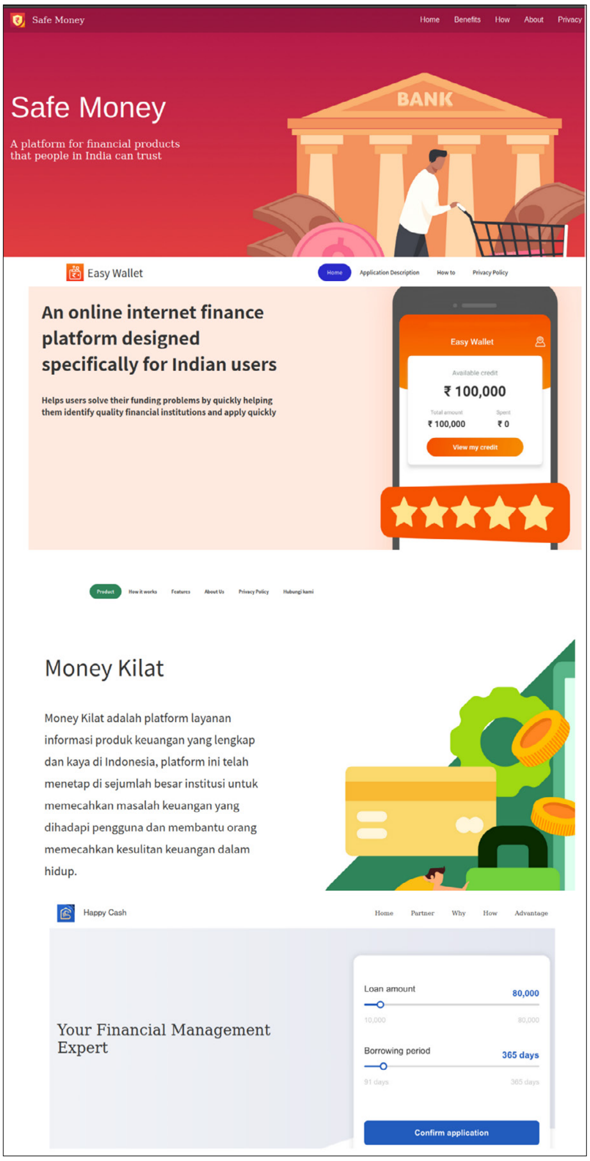
Urgent❗Important❗Notice from 【YesCash】loan association❗Dear users, your loan in【YesCash】has expired, please pay in time to avoid overdue. If it is overdue, the system will automatically contact your family and friends, and the loan will increase the penalty and put more burden on you. More seriously, those with serious circumstances will be prosecuted and sanctioned by law.

Figure 14: Message threatening legal action and threatening to contact family and friends.

WEB INFRASTRUCTURE

In an attempt to appear legitimate, these loan apps have websites providing basic information. The template of the website may vary based on the country, but they all contain a logo, menu, and basic information, including a privacy page.

The hosting sites of the websites we found varied, but many of those we encountered were hosted at *Alibaba* cloud and some on *Amazon Web Services*.



Safe Money

A platform for financial products that people in India can trust

An online internet finance platform designed specifically for Indian users

Helps users solve their funding problems by quickly helping them identify quality financial institutions and apply quickly

Money Kilat

Money Kilat adalah platform layanan informasi produk keuangan yang lengkap dan kaya di Indonesia, platform ini telah menetap di sejumlah besar institusi untuk memecahkan masalah keuangan yang dihadapi pengguna dan membantu orang memecahkan kesulitan keuangan dalam hidup.

Your Financial Management Expert

Loan amount 80,000

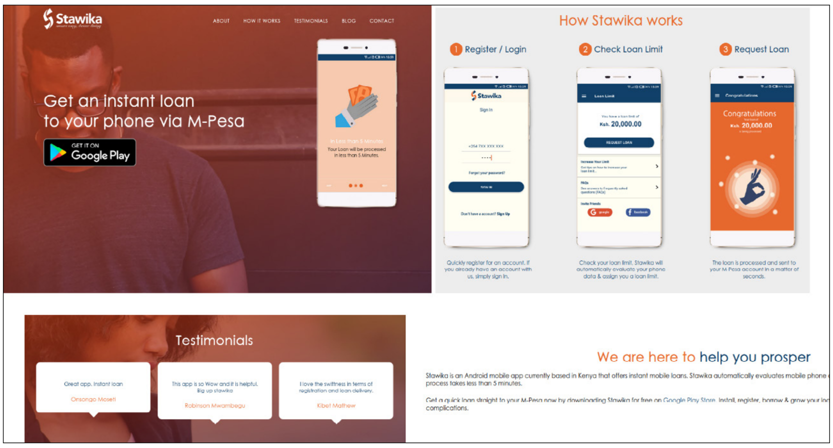
10,000 80,000

Borrowing period 365 days

91 days 365 days

Figure 15: Loan app websites.

Not all the websites have direct links to download the app, probably out of fear of the app being removed from the app platform. Some of the apps only have the website to convince users, and probably app reviewers, usually linked with a reference from the app platform page.



Get an instant loan to your phone via M-Pesa

How Stawika works

Quickly register for an account. If you already have an account with us, simply sign in.

Check your loan limit. Stawika will automatically evaluate your phone data & assign you a loan limit.

The loan is processed and sent to your M Pesa account in a matter of seconds.

Great app. Instant loan

Onsongo Moseti

This app is so Wow and it is helpful. Big up stawika

Robinson Mwambegu

I love the swiftness in terms of registration and loan delivery.

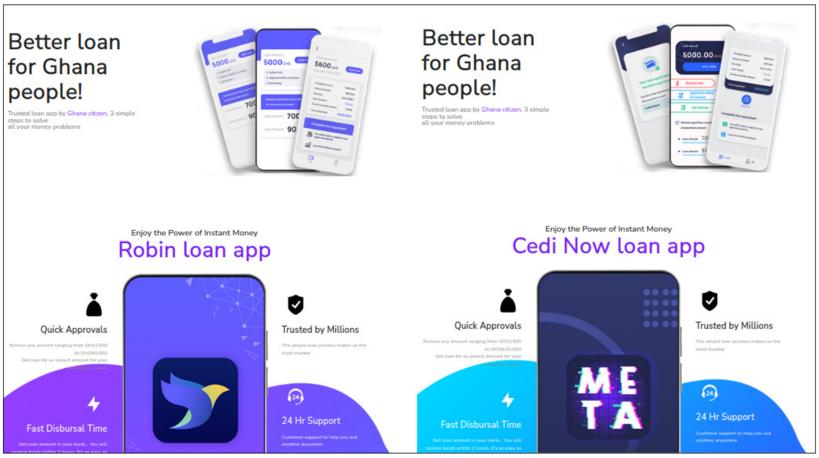
Kibet Mathew

We are here to help you prosper

Stawika is an Android mobile app currently based in Kenya that offers instant mobile loans. Stawika automatically evaluates mobile phone process takes less than 5 minutes.

Get a quick loan straight to your M-Pesa now by downloading Stawika for free on Google Play Store. Install, register, borrow & grow your lo complications.

Figure 16: Stawika loan app website.



Better loan for Ghana people!

Trusted loan app by Ghana citizen, 3 simple steps to solve all your money problems

Better loan for Ghana people!

Trusted loan app by Ghana citizen, 3 simple steps to solve all your money problems

Enjoy the Power of Instant Money

Robin loan app

Borrow any amount ranging from GHS1500 to GHS60,000 Get loan for as lowest amount for your emergency needs

The simple loan process makes us the most trusted

Get loan amount in your bank, You will receive funds within 2 hours. It's as easy as

Customer support to help you out anytime anywhere

Enjoy the Power of Instant Money

Cedi Now loan app

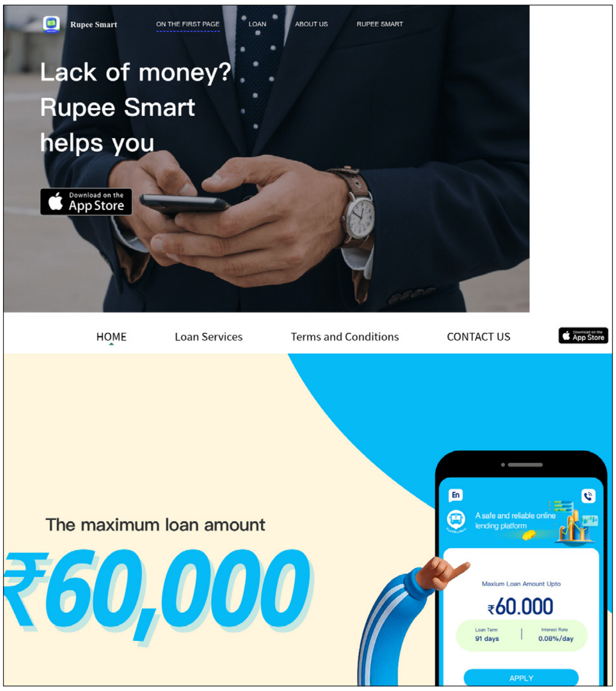
Borrow any amount ranging from GHS1500 to GHS6,00,000 Get loan for as lowest amount for your emergency needs

The simple loan process makes us the most trusted

Get loan amount in your bank, You will receive funds within 2 hours. It's as easy as

Customer support to help you out anytime anywhere

Figure 17: Loan app websites with similar templates targeting users in Ghana.

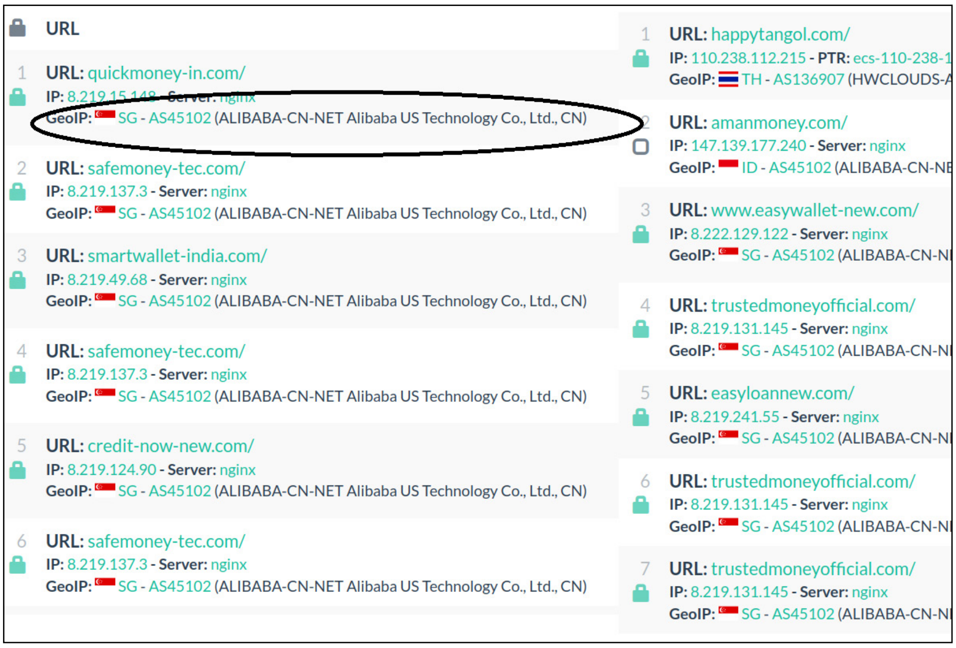


Lack of money? Rupee Smart helps you

The maximum loan amount

₹60,000

Figure 18: iOS App Store app distribution sites.



URL

1 URL: quickmoney-in.com/
IP: 8.219.15.148 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

2 URL: safemoney-tec.com/
IP: 8.219.137.3 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

3 URL: smartwallet-india.com/
IP: 8.219.49.68 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

4 URL: safemoney-tec.com/
IP: 8.219.137.3 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

5 URL: credit-now-new.com/
IP: 8.219.124.90 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

6 URL: safemoney-tec.com/
IP: 8.219.137.3 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN)

1 URL: happytangol.com/
IP: 110.238.112.215 - PTR: ecs-110-238-1
GeoIP: TH - AS136907 (HWCLOUDS-A

2 URL: amanmoney.com/
IP: 147.139.177.240 - Server: nginx
GeoIP: ID - AS45102 (ALIBABA-CN-NE

3 URL: www.easywallet-new.com/
IP: 8.222.129.122 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NI

4 URL: trustedmoneyofficial.com/
IP: 8.219.131.145 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NI

5 URL: easyloannew.com/
IP: 8.219.241.55 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NI

6 URL: trustedmoneyofficial.com/
IP: 8.219.131.145 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NI

7 URL: trustedmoneyofficial.com/
IP: 8.219.131.145 - Server: nginx
GeoIP: SG - AS45102 (ALIBABA-CN-NI

Figure 19: We found several spyware instant loan app websites hosted at Alibaba.

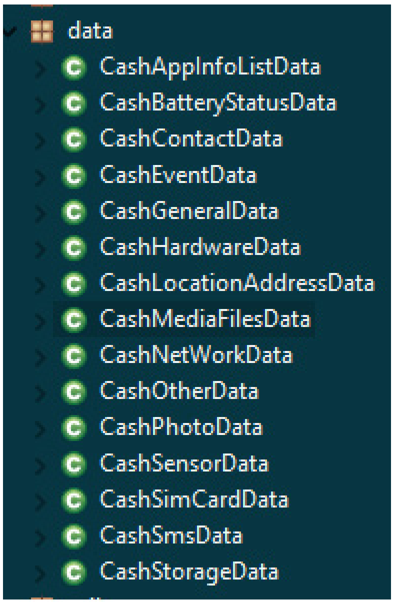
APP ANALYSIS

There are a wide variety of spyware loan app samples. The critical part of these apps is accessing sensitive data; we can group them into different categories based on how they get this data. We'll discuss some of them here.

Data access

Hash: 181f3d34f86b1c27136177a31186f0a70ba5565b6c9a6e4e5e055ba5ce35caf8

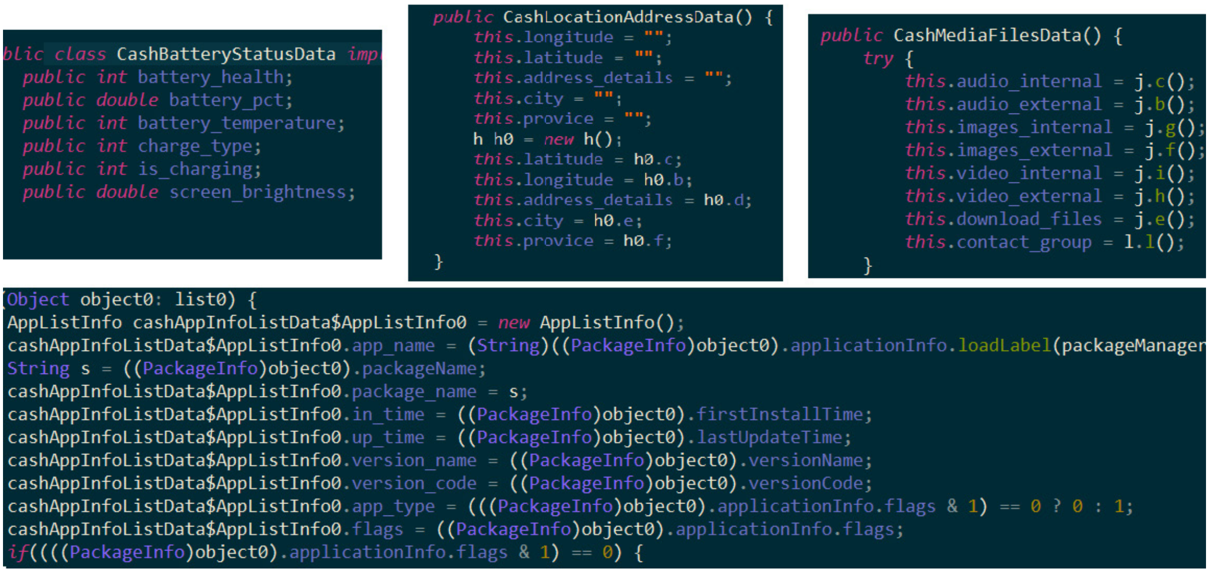
Lots of apps access data in a standard way without any concealment. We'll go through the code snippets of one such app. This app gives a good representation of the amount of data that is collected. Looking at the code snippets, it is flabbergasting to see the finer details of the data collected and imagine what the fraudsters can do with that amount of data – you will quickly understand why we call this 'data espionage'.



data
CashAppInfoListData
CashBatteryStatusData
CashContactData
CashEventData
CashGeneralData
CashHardwareData
CashLocationAddressData
CashMediaFilesData
CashNetWorkData
CashOtherData
CashPhotoData
CashSensorData
CashSimCardData
CashSmsData
CashStorageData

Figure 20: The class names give an idea of the variety of data collected.

App data, such as a list of applications on the device, the install time, versions, and app types, is collected. Battery status, the level of battery, temperature, and brightness are collected. Besides that, location details, audio, video, and file download lists are collected.



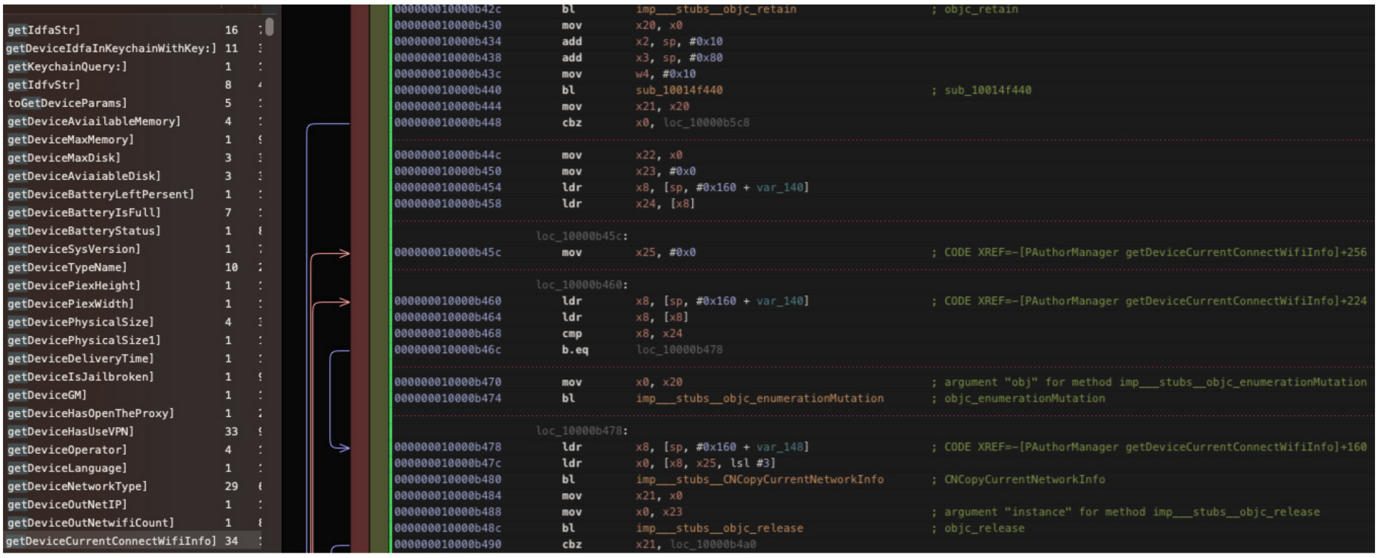
```
blic class CashBatteryStatusData imp
  public int battery_health;
  public double battery_pct;
  public int battery_temperature;
  public int charge_type;
  public int is_charging;
  public double screen_brightness;
```

```
public CashLocationAddressData() {
    this.longitude = "";
    this.latitude = "";
    this.address_details = "";
    this.city = "";
    this.provice = "";
    h h0 = new h();
    this.latitude = h0.c;
    this.longitude = h0.b;
    this.address_details = h0.d;
    this.city = h0.e;
    this.provice = h0.f;
}
```

```
public CashMediaFilesData() {
    try {
        this.audio_internal = j.c();
        this.audio_external = j.b();
        this.images_internal = j.g();
        this.images_external = j.f();
        this.video_internal = j.i();
        this.video_external = j.h();
        this.download_files = j.e();
        this.contact_group = l.l();
    }
```

```
Object object0: list0) {
AppListInfo cashAppInfoListData$AppListInfo0 = new AppListInfo();
cashAppInfoListData$AppListInfo0.app_name = (String)((PackageInfo)object0).applicationInfo.loadLabel(packageManager
String s = ((PackageInfo)object0).packageName;
cashAppInfoListData$AppListInfo0.package_name = s;
cashAppInfoListData$AppListInfo0.in_time = ((PackageInfo)object0).firstInstallTime;
cashAppInfoListData$AppListInfo0.up_time = ((PackageInfo)object0).lastUpdateTime;
cashAppInfoListData$AppListInfo0.version_name = ((PackageInfo)object0).versionName;
cashAppInfoListData$AppListInfo0.version_code = ((PackageInfo)object0).versionCode;
cashAppInfoListData$AppListInfo0.app_type = (((PackageInfo)object0).applicationInfo.flags & 1) == 0 ? 0 : 1;
cashAppInfoListData$AppListInfo0.flags = ((PackageInfo)object0).applicationInfo.flags;
if((((PackageInfo)object0).applicationInfo.flags & 1) == 0) {
```

Figure 21: Code snippet showing app list, battery status, location and media files data collection.

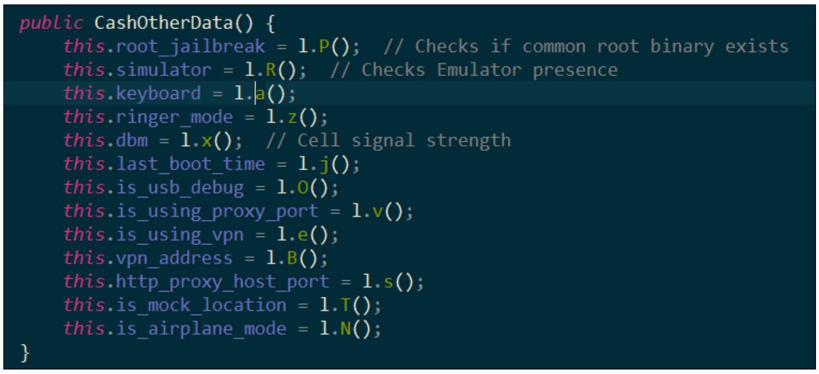


```
getIdfaStr]                        16
getDeviceIdfaInKeychainWithKey:]   11
getKeychainQuery:]                 1
getIdfvStr]                        8
toGetDeviceParams]                 5
getDeviceAviailableMemory]         4
getDeviceMaxMemory]                1
getDeviceMaxDisk]                  3
getDeviceAviaiableDisk]            3
getDeviceBatteryLeftPersent]       1
getDeviceBatteryIsFull]            7
getDeviceBatteryStatus]            1
getDeviceSysVersion]               1
getDeviceTypeName]                 10
getDevicePiexHeight]               1
getDevicePiexWidth]                1
getDevicePhysicalSize]             4
getDevicePhysicalSize1]            1
getDeviceDeliveryTime]             1
getDeviceIsJailbroken]             1
getDeviceGM]                       1
getDeviceHasOpenTheProxy]          1
getDeviceHasUseVPN]                33
getDeviceOperator]                 4
getDeviceLanguage]                 1
getDeviceNetworkType]              29
getDeviceOutNetIP]                 1
getDeviceOutNetwifiCount]          1
getDeviceCurrentConnectWifiInfo]   34
```

```
000000010000b42c    bl      imp___stubs__objc_retain                   ; objc_retain
000000010000b430    mov     x20, x0
000000010000b434    add     x2, sp, #0x10
000000010000b438    add     x3, sp, #0x80
000000010000b43c    mov     w4, #0x10
000000010000b440    bl      sub_10014f440                              ; sub_10014f440
000000010000b444    mov     x21, x20
000000010000b448    cbz     x0, loc_10000b5c8

000000010000b44c    mov     x22, x0
000000010000b450    mov     x23, #0x0
000000010000b454    ldr     x8, [sp, #0x160 + var_140]
000000010000b458    ldr     x24, [x8]

                loc_10000b45c:
000000010000b45c    mov     x25, #0x0                                  ; CODE XREF=-[PAuthorManager getDeviceCurrentConnectWifiInfo]+256

                loc_10000b460:
000000010000b460    ldr     x8, [sp, #0x160 + var_140]                 ; CODE XREF=-[PAuthorManager getDeviceCurrentConnectWifiInfo]+224
000000010000b464    ldr     x8, [x8]
000000010000b468    cmp     x8, x24
000000010000b46c    b.eq    loc_10000b478

000000010000b470    mov     x0, x20                                    ; argument "obj" for method imp___stubs__objc_enumerationMutation
000000010000b474    bl      imp___stubs__objc_enumerationMutation      ; objc_enumerationMutation

                loc_10000b478:
000000010000b478    ldr     x8, [sp, #0x160 + var_148]                 ; CODE XREF=-[PAuthorManager getDeviceCurrentConnectWifiInfo]+160
000000010000b47c    ldr     x0, [x8, x25, lsl #3]
000000010000b480    bl      imp___stubs__CNCopyCurrentNetworkInfo      ; CNCopyCurrentNetworkInfo
000000010000b484    mov     x21, x0
000000010000b488    mov     x0, x23                                    ; argument "instance" for method imp___stubs__objc_release
000000010000b48c    bl      imp___stubs__objc_release                  ; objc_release
000000010000b490    cbz     x21, loc_10000b4a0
```

Figure 22: iOS code snippet.

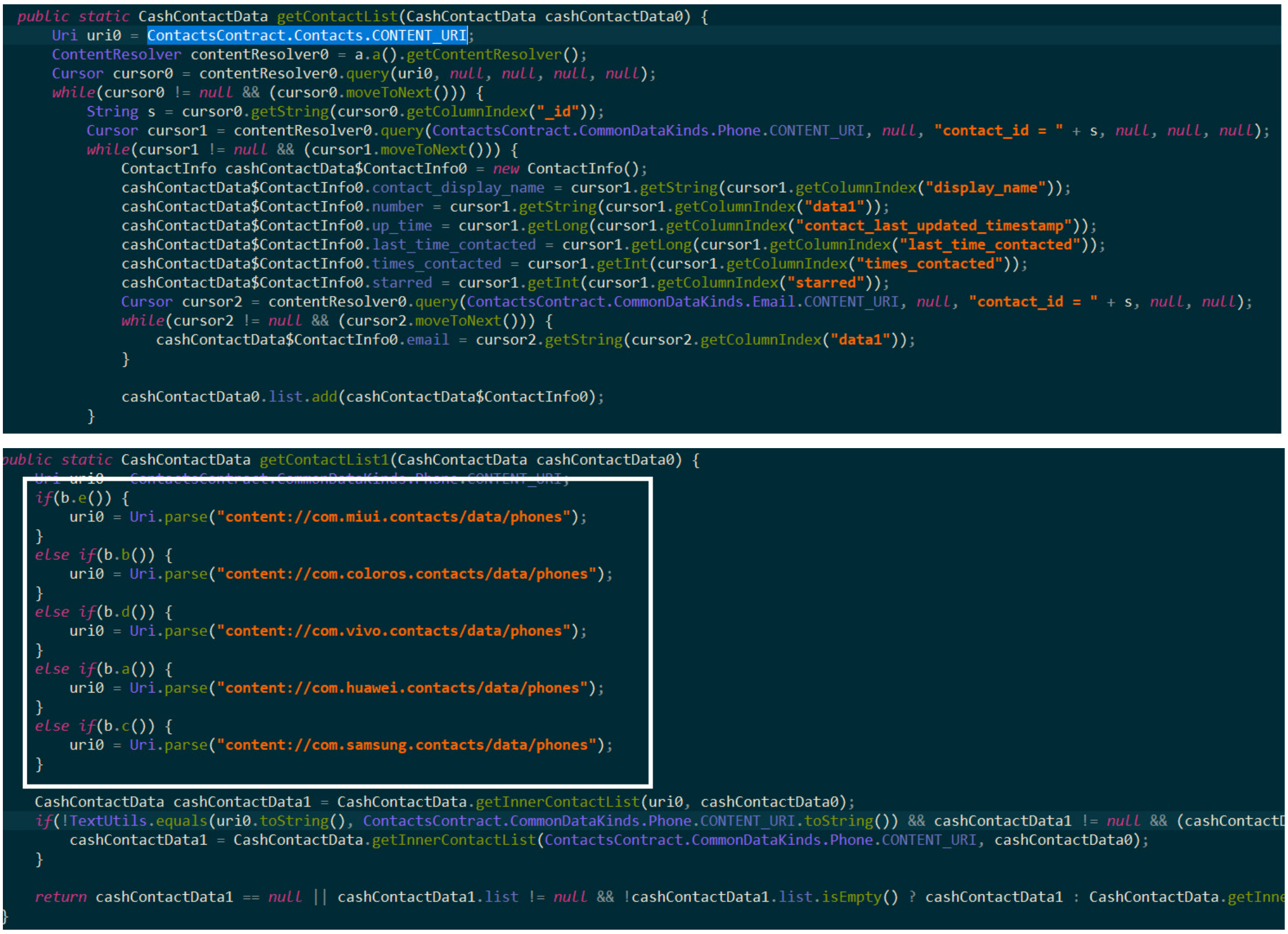
The app also checks if the device is rooted, by checking if the well-known root binary file exists; it will also check if it's running on an emulator, genymotion, etc.; it checks signal strength, VPN, proxy, mock location, and keyboard type, probably to verify if it is being run by researchers – which is definitely not something a loan application should do.



```
public CashOtherData() {
    this.root_jailbreak = l.P();  // Checks if common root binary exists
    this.simulator = l.R();  // Checks Emulator presence
    this.keyboard = l.a();
    this.ringer_mode = l.z();
    this.dbm = l.x();  // Cell signal strength
    this.last_boot_time = l.j();
    this.is_usb_debug = l.O();
    this.is_using_proxy_port = l.v();
    this.is_using_vpn = l.e();
    this.vpn_address = l.B();
    this.http_proxy_host_port = l.s();
    this.is_mock_location = l.T();
    this.is_airplane_mode = l.N();
}
```

Figure 23: Code snippet to check more device-specific data.

The app extracts the display name, number, last updated time stamp, times they were contacted, and if it was starred by querying the ContactsContract content. For specific phones, such as those widely used in Asia like *Xiaomi* (*Miui*), *Samsung*, *Huawei*, *Vivo* and *Coloros*, they look for specific locations to extract contact content.

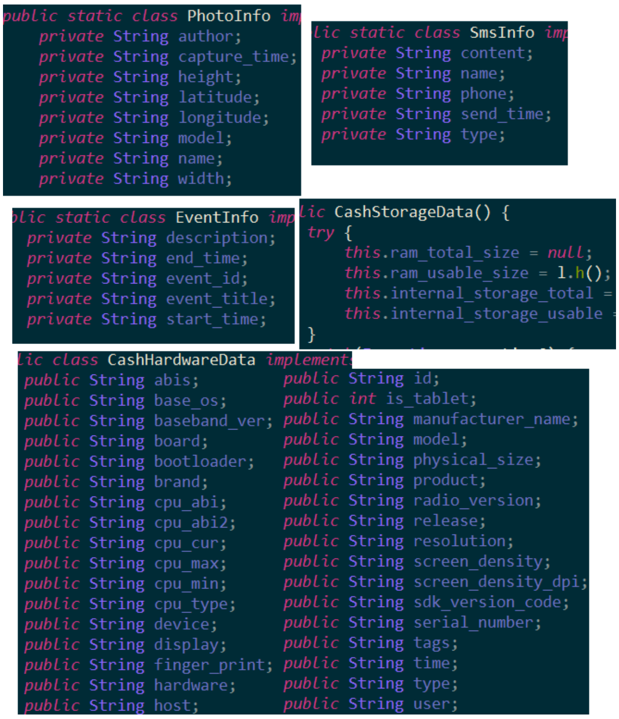


```
public static CashContactData getContactList(CashContactData cashContactData0) {
    Uri uri0 = ContactsContract.Contacts.CONTENT_URI;
    ContentResolver contentResolver0 = a.a().getContentResolver();
    Cursor cursor0 = contentResolver0.query(uri0, null, null, null, null);
    while(cursor0 != null && (cursor0.moveToNext())) {
        String s = cursor0.getString(cursor0.getColumnIndex("_id"));
        Cursor cursor1 = contentResolver0.query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, null, "contact_id = " + s, null, null, null);
        while(cursor1 != null && (cursor1.moveToNext())) {
            ContactInfo cashContactData$ContactInfo0 = new ContactInfo();
            cashContactData$ContactInfo0.contact_display_name = cursor1.getString(cursor1.getColumnIndex("display_name"));
            cashContactData$ContactInfo0.number = cursor1.getString(cursor1.getColumnIndex("data1"));
            cashContactData$ContactInfo0.up_time = cursor1.getLong(cursor1.getColumnIndex("contact_last_updated_timestamp"));
            cashContactData$ContactInfo0.last_time_contacted = cursor1.getLong(cursor1.getColumnIndex("last_time_contacted"));
            cashContactData$ContactInfo0.times_contacted = cursor1.getInt(cursor1.getColumnIndex("times_contacted"));
            cashContactData$ContactInfo0.starred = cursor1.getInt(cursor1.getColumnIndex("starred"));
            Cursor cursor2 = contentResolver0.query(ContactsContract.CommonDataKinds.Email.CONTENT_URI, null, "contact_id = " + s, null, null);
            while(cursor2 != null && (cursor2.moveToNext())) {
                cashContactData$ContactInfo0.email = cursor2.getString(cursor2.getColumnIndex("data1"));
            }

            cashContactData0.list.add(cashContactData$ContactInfo0);
        }
```

```
public static CashContactData getContactList1(CashContactData cashContactData0) {
    ~~Uri uri0 = ContactsContract.CommonDataKinds.Phone.CONTENT_URI;~~
    if(b.e()) {
        uri0 = Uri.parse("content://com.miui.contacts/data/phones");
    }
    else if(b.b()) {
        uri0 = Uri.parse("content://com.coloros.contacts/data/phones");
    }
    else if(b.d()) {
        uri0 = Uri.parse("content://com.vivo.contacts/data/phones");
    }
    else if(b.a()) {
        uri0 = Uri.parse("content://com.huawei.contacts/data/phones");
    }
    else if(b.c()) {
        uri0 = Uri.parse("content://com.samsung.contacts/data/phones");
    }

    CashContactData cashContactData1 = CashContactData.getInnerContactList(uri0, cashContactData0);
    if(!TextUtils.equals(uri0.toString(), ContactsContract.CommonDataKinds.Phone.CONTENT_URI.toString()) && cashContactData1 != null && (cashContactD
        cashContactData1 = CashContactData.getInnerContactList(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, cashContactData0);
    }

    return cashContactData1 == null || cashContactData1.list != null && !cashContactData1.list.isEmpty() ? cashContactData1 : CashContactData.getInne
}
```

Figure 24: Code snippet of contact list data collection.

They collect extensive hardware data, including manufacturer, screen details, CPU details and bootloader. They will also collect events data and SMS messages from the OS, as shown in the code snippet in Figure 25.



```
public static class PhotoInfo im
    private String author;
    private String capture_time;
    private String height;
    private String latitude;
    private String longitude;
    private String model;
    private String name;
    private String width;
```

```
lic static class SmsInfo imp
 private String content;
 private String name;
 private String phone;
 private String send_time;
 private String type;
```

```
blic static class EventInfo imp
  private String description;
  private String end_time;
  private String event_id;
  private String event_title;
  private String start_time;
```

```
lic CashStorageData() {
try {
    this.ram_total_size = null;
    this.ram_usable_size = l.h();
    this.internal_storage_total =
    this.internal_storage_usable =
}
```

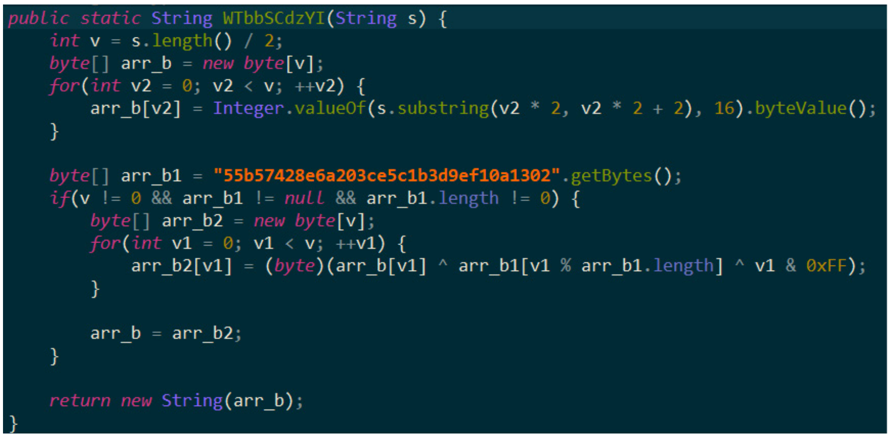
```
lic class CashHardwareData implement
public String abis;          public String id;
public String base_os;       public int is_tablet;
public String baseband_ver;  public String manufacturer_name;
public String board;         public String model;
public String bootloader;    public String physical_size;
public String brand;         public String product;
public String cpu_abi;       public String radio_version;
public String cpu_abi2;      public String release;
public String cpu_cur;       public String resolution;
public String cpu_max;       public String screen_density;
public String cpu_min;       public String screen_density_dpi;
public String cpu_type;      public String sdk_version_code;
public String device;        public String serial_number;
public String display;       public String tags;
public String finger_print;  public String time;
public String hardware;      public String type;
public String host;          public String user;
```

Figure 25: Code snippet showing type of photo, hardware, storage and SMS data collected.

Encoding

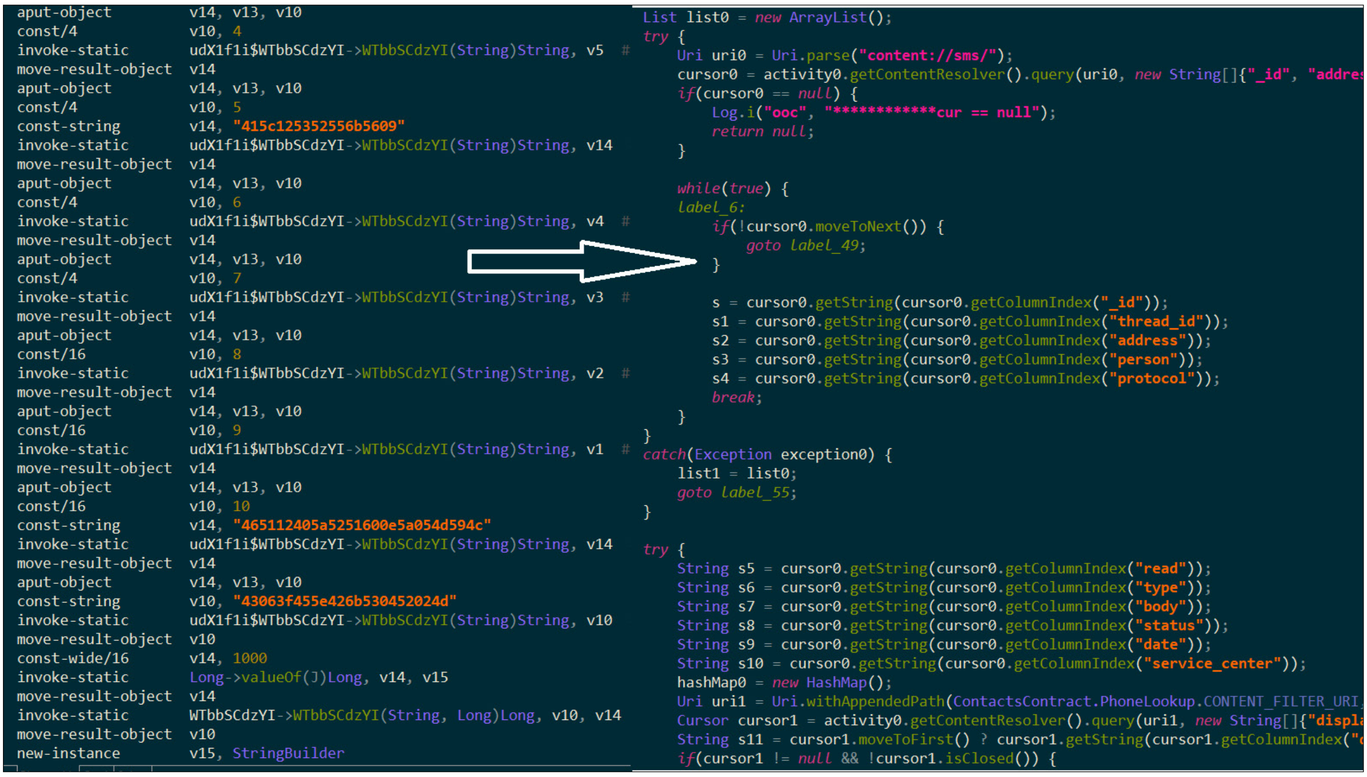
Hash: 2717fd8e04251ba5b1315a28efa0713d523bde87c58da798831124e13c15de1a

Some applications encode the key strings related to the data extraction from the device. Encoding routines are used, and some of these routines are shared across several samples, indicating the same author or group behind the development.



```
public static String WTbbSCdzYI(String s) {
    int v = s.length() / 2;
    byte[] arr_b = new byte[v];
    for(int v2 = 0; v2 < v; ++v2) {
        arr_b[v2] = Integer.valueOf(s.substring(v2 * 2, v2 * 2 + 2), 16).byteValue();
    }

    byte[] arr_b1 = "55b57428e6a203ce5c1b3d9ef10a1302".getBytes();
    if(v != 0 && arr_b1 != null && arr_b1.length != 0) {
        byte[] arr_b2 = new byte[v];
        for(int v1 = 0; v1 < v; ++v1) {
            arr_b2[v1] = (byte)(arr_b[v1] ^ arr_b1[v1 % arr_b1.length] ^ v1 & 0xFF);
        }

        arr_b = arr_b2;
    }

    return new String(arr_b);
}
```

Figure 26: Encoded code snippet.



```
aput-object         v14, v13, v10
const/4             v10, 4
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v5  #
move-result-object  v14
aput-object         v14, v13, v10
const/4             v10, 5
const-string        v14, "415c125352556b5609"
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v14
move-result-object  v14
aput-object         v14, v13, v10
const/4             v10, 6
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v4  #
move-result-object  v14
aput-object         v14, v13, v10
const/4             v10, 7
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v3  #
move-result-object  v14
aput-object         v14, v13, v10
const/16            v10, 8
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v2  #
move-result-object  v14
aput-object         v14, v13, v10
const/16            v10, 9
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v1  #
move-result-object  v14
aput-object         v14, v13, v10
const/16            v10, 10
const-string        v14, "465112405a5251600e5a054d594c"
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v14
move-result-object  v14
aput-object         v14, v13, v10
const-string        v10, "43063f455e426b530452024d"
invoke-static       udX1f1i$WTbbSCdzYI->WTbbSCdzYI(String)String, v10
move-result-object  v10
const-wide/16       v14, 1000
invoke-static       Long->valueOf(J)Long, v14, v15
move-result-object  v14
invoke-static       WTbbSCdzYI->WTbbSCdzYI(String, Long)Long, v10, v14
move-result-object  v10
new-instance        v15, StringBuilder
```

```
List list0 = new ArrayList();
try {
    Uri uri0 = Uri.parse("content://sms/");
    cursor0 = activity0.getContentResolver().query(uri0, new String[]{"_id", "addre
    if(cursor0 == null) {
        Log.i("ooc", "************cur == null");
        return null;
    }

    while(true) {
    label_6:
        if(!cursor0.moveToNext()) {
            goto label_49;
        }

        s = cursor0.getString(cursor0.getColumnIndex("_id"));
        s1 = cursor0.getString(cursor0.getColumnIndex("thread_id"));
        s2 = cursor0.getString(cursor0.getColumnIndex("address"));
        s3 = cursor0.getString(cursor0.getColumnIndex("person"));
        s4 = cursor0.getString(cursor0.getColumnIndex("protocol"));
        break;
    }
}
catch(Exception exception0) {
    list1 = list0;
    goto label_55;
}

try {
    String s5 = cursor0.getString(cursor0.getColumnIndex("read"));
    String s6 = cursor0.getString(cursor0.getColumnIndex("type"));
    String s7 = cursor0.getString(cursor0.getColumnIndex("body"));
    String s8 = cursor0.getString(cursor0.getColumnIndex("status"));
    String s9 = cursor0.getString(cursor0.getColumnIndex("date"));
    String s10 = cursor0.getString(cursor0.getColumnIndex("service_center"));
    hashMap0 = new HashMap();
    Uri uri1 = Uri.withAppendedPath(ContactsContract.PhoneLookup.CONTENT_FILTER_URI,
    Cursor cursor1 = activity0.getContentResolver().query(uri1, new String[]{"displa
    String s11 = cursor1.moveToFirst() ? cursor1.getString(cursor1.getColumnIndex("
    if(cursor1 != null && !cursor1.isClosed()) {
```

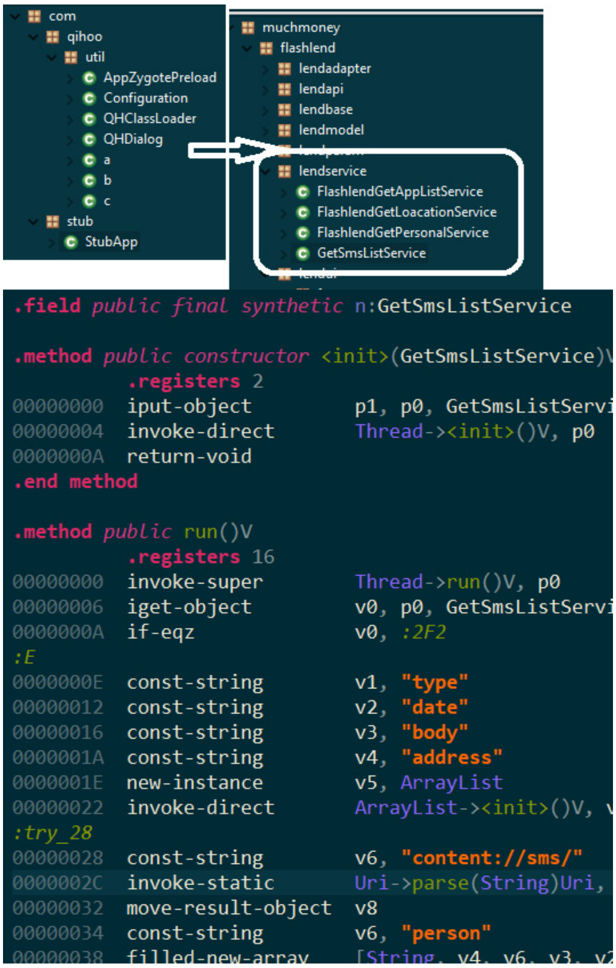
Figure 27: Encoded app code snippet.

Packed samples

Hash: e8e9866de70ce17c547c2541fd5a24fdbbe7cbc5e7f49b8e6a2aaff867ca4aa5

Packing is a known technique used to delay the analysis of an application. We encountered Jiagu-packed samples. Jiagu is a known packer used in the *Play Store* by both malicious and clean apps, and it is popular in Asia. These apps declare that they collect your data. The reason for using a packer could be to stop competitors from stealing code or to make it less obvious to researchers and reviewers that the app contains sensitive data collection code.

Other than Jiagu, we also noticed samples packed with the package com.proxy.shellapplication, and other researchers have spotted samples built with the Flutter framework [8].

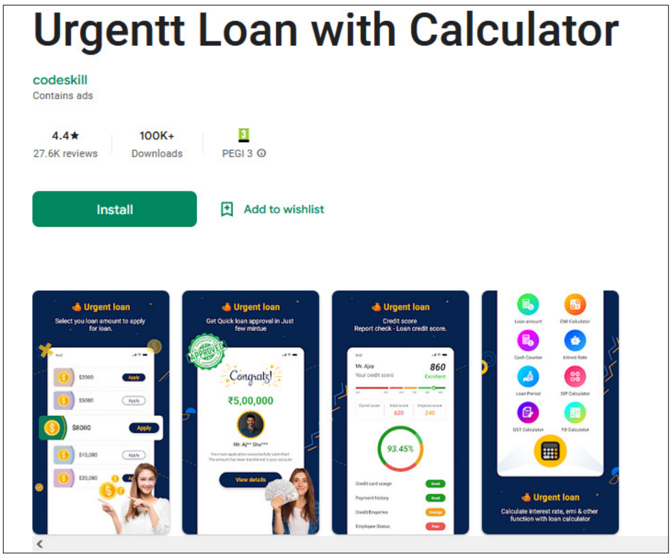


```
.field public final synthetic n:GetSmsListService

.method public constructor <init>(GetSmsListService)V
          .registers 2
00000000  iput-object          p1, p0, GetSmsListServi
00000004  invoke-direct        Thread-><init>()V, p0
0000000A  return-void
.end method

.method public run()V
          .registers 16
00000000  invoke-super         Thread->run()V, p0
00000006  iget-object          v0, p0, GetSmsListServi
0000000A  if-eqz               v0, :2F2
:E
0000000E  const-string         v1, "type"
00000012  const-string         v2, "date"
00000016  const-string         v3, "body"
0000001A  const-string         v4, "address"
0000001E  new-instance         v5, ArrayList
00000022  invoke-direct        ArrayList-><init>()V, v
:try_28
00000028  const-string         v6, "content://sms/"
0000002C  invoke-static        Uri->parse(String)Uri,
00000032  move-result-object   v8
00000034  const-string         v6, "person"
00000038  filled-new-array     [String, v4, v6, v3, v2
```

Figure 28: Jiagu packed vs unpacked.

INSTANT LOAN ADWARE THAT FEEDS ON FRENZY

Some instant loan apps claim to provide instant loans but do not actually provide any loans and exist only to serve advertisements. The 'Urgentt Loan with Calculator' [9] app, when launched, opens with an advertisement; it doesn't offer any loans itself. When you click on anything, it pops out an advertisement or wants you to click a redirect to another application, making its money through advertisements and pay-per-install. Urgentt Loan with Calculator is just one example; over the years, several apps like these have appeared in the app stores.

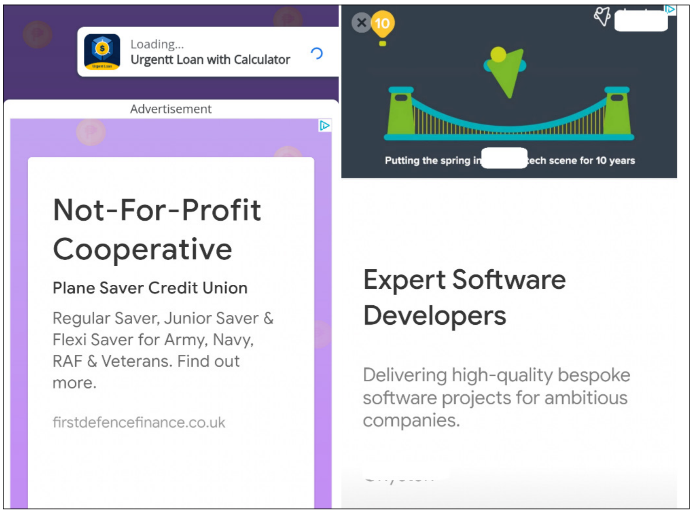

Urgentt Loan with Calculator

codeskill
Contains ads

4.4★ 27.6K reviews | 100K+ Downloads | PEGI 3

Install
Add to wishlist
Urgent loan
Select you loan amount to apply for loan.
Get Quick loan approval in Just few mintue
Congrats!
₹5,00,000
Credit score
Report check - Loan credit score.
860
93.45%
Calculate interest rate, emi & other function with loan calculator

Figure 29: Play store page for advertisement app.



Loading...
Urgentt Loan with Calculator

Advertisement

Not-For-Profit Cooperative

Plane Saver Credit Union

Regular Saver, Junior Saver & Flexi Saver for Army, Navy, RAF & Veterans. Find out more.

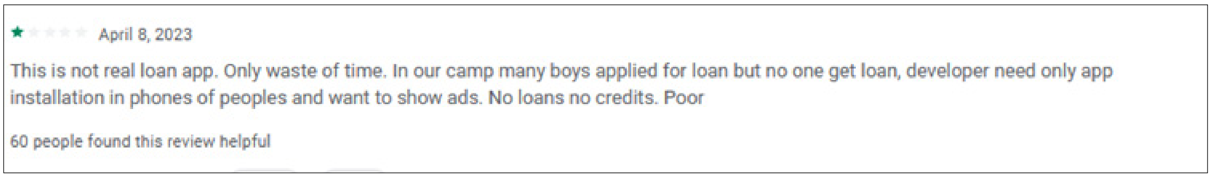
firstdefencefinance.co.uk

Putting the spring in [redacted] tech scene for 10 years

Expert Software Developers

Delivering high-quality bespoke software projects for ambitious companies.

Figure 30: Urgentt Loan with Calculator advertisements display.



★☆☆☆☆ April 8, 2023

This is not real loan app. Only waste of time. In our camp many boys applied for loan but no one get loan, developer need only app installation in phones of peoples and want to show ads. No loans no credits. Poor

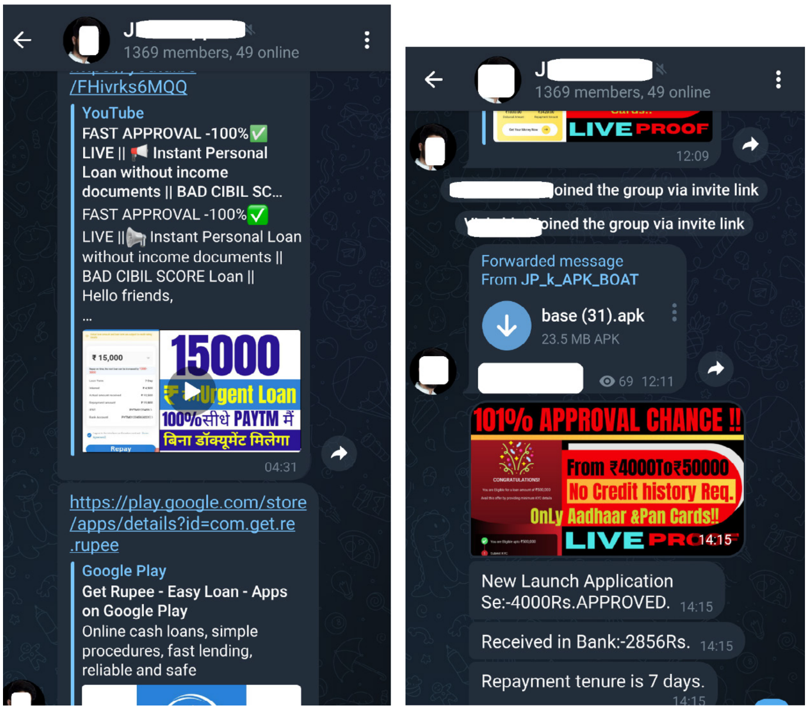
60 people found this review helpful

Figure 31: User review confirming that it's only an advert app without any loans.

HOW ARE THEY DISTRIBUTED?

Telegram and Facebook groups

Borrowers are targeted using *Telegram* and *Facebook* groups. They advertise, post reviews, and comment on social media promoting these groups. Then they have the target audience to distribute what they like. Increasingly, personal loan apps are distributed on the *Play Store*. When the apps were removed from the app platforms, we noticed that they started distributing APKs directly through the platform.



J[redacted]
1369 members, 49 online

/FHivrks6MQQ

YouTube
FAST APPROVAL -100%✅ LIVE || 📢 Instant Personal Loan without income documents || BAD CIBIL SC...
FAST APPROVAL -100%✅ LIVE ||📢 Instant Personal Loan without income documents || BAD CIBIL SCORE Loan || Hello friends,
...

04:31

https://play.google.com/store/apps/details?id=com.get.re.rupee

Google Play
Get Rupee - Easy Loan - Apps on Google Play
Online cash loans, simple procedures, fast lending, reliable and safe

J[redacted]
1369 members, 49 online

12:09

[redacted] joined the group via invite link

[redacted] joined the group via invite link

Forwarded message
From JP_k_APK_BOAT
base (31).apk
23.5 MB APK
[redacted] 69 12:11

14:15

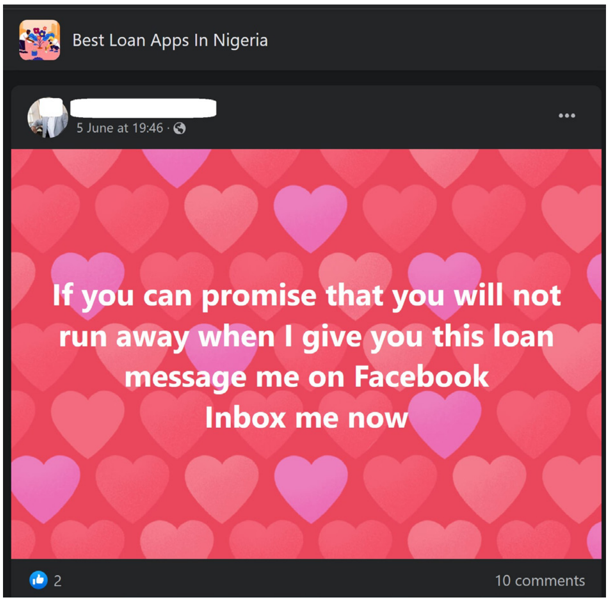
New Launch Application Se:-4000Rs.APPROVED. 14:15

Received in Bank:-2856Rs. 14:15

Repayment tenure is 7 days. 14:15

Figure 32: Telegram groups promoting personal loan apps.

The crooks behind these apps know that their target audience spends time on social media sites, so they have several *Facebook* groups and *Facebook* pages to promote them. They create these sources with the message that the loan will be instant and without credit checks. This will attract the attention of those who need a loan or who have been rejected by traditional banks due to a lack of paperwork or a poor credit report.

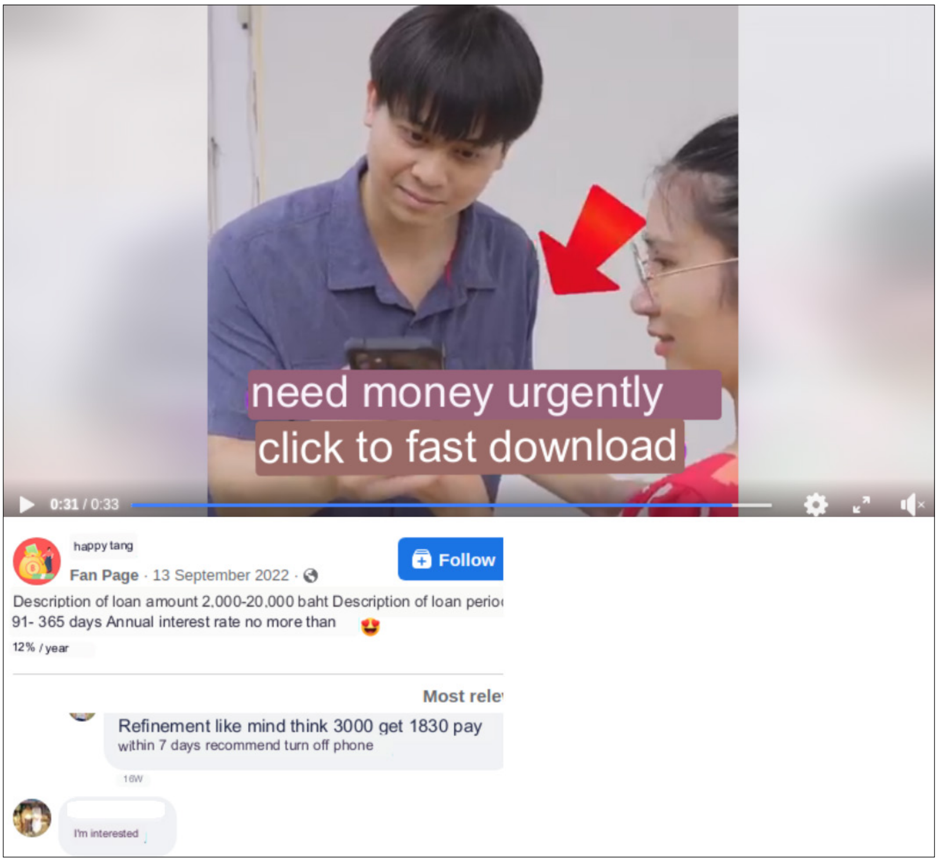


Best Loan Apps In Nigeria

[redacted]
5 June at 19:46 ·

If you can promise that you will not run away when I give you this loan message me on Facebook Inbox me now

Figure 33: Luring potential victims through Facebook groups.



need money urgently
click to fast download

happy tang
Fan Page · 13 September 2022 ·

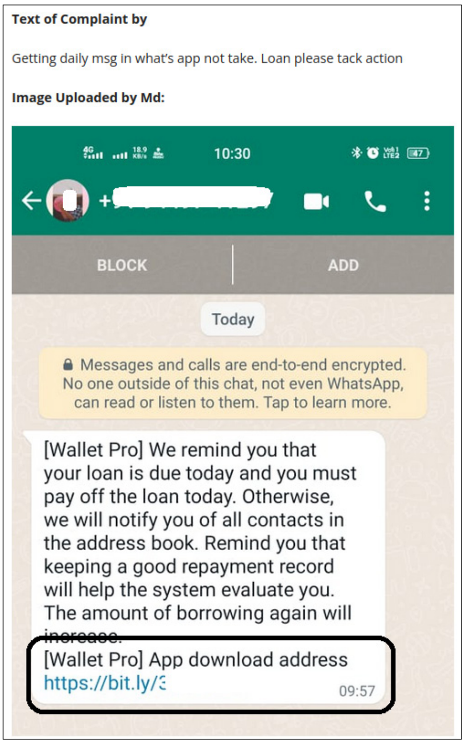
Description of loan amount 2,000-20,000 baht Description of loan perio
91- 365 days Annual interest rate no more than 😍
12% / year

Refinement like mind think 3000 get 1830 pay
within 7 days recommend turn off phone
16W

[redacted]
I'm interested

Figure 34: Thai (translated) loan app being driven through the Facebook page video promotion.

We found some users complaining that they had never taken a loan, but they were still sent threatening messages and a link to download the app. We highly suspect that these people's phone numbers were targeted using data from the contact lists that crooks obtained illegally from borrowers. When they send these messages, they threaten to force installation and borrowing on potential new victims.



Text of Complaint by

Getting daily msg in what's app not take. Loan please tack action

Image Uploaded by Md:

10:30

+[redacted]

BLOCK | ADD

Today

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

[Wallet Pro] We remind you that your loan is due today and you must pay off the loan today. Otherwise, we will notify you of all contacts in the address book. Remind you that keeping a good repayment record will help the system evaluate you. The amount of borrowing again will increase.

[Wallet Pro] App download address https://bit.ly/3 09:57

Figure 35: Data abuse to threaten and distribute apps to phone numbers collected from previous borrowers.

Ads and SMS messages

Traditional methods such as sending SMS and advertising on social media such as *Twitter* and *YouTube* are also used to entice users to install these apps.

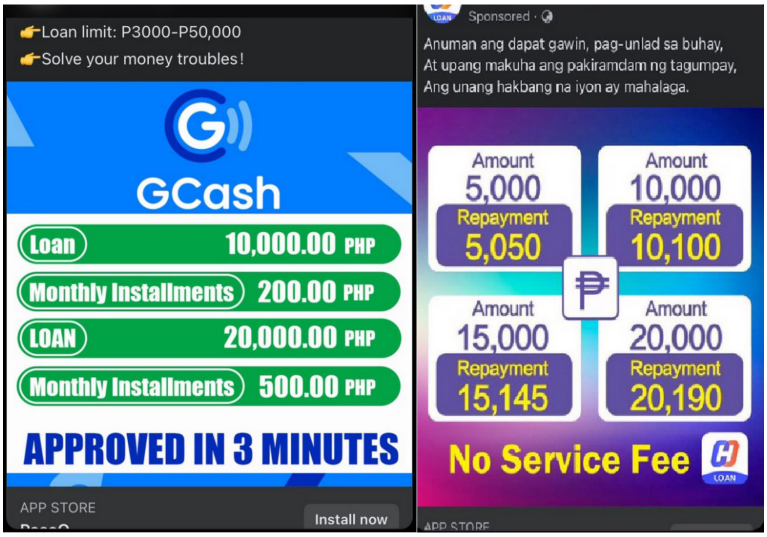
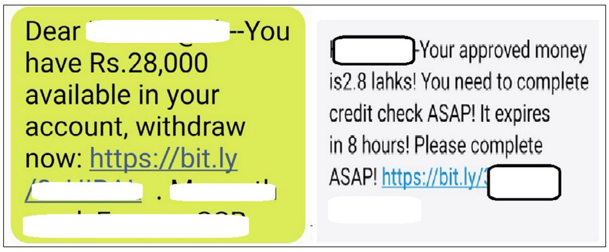

👉Loan limit: P3000-P50,000
👉Solve your money troubles!
GCash
Loan 10,000.00 PHP
Monthly Installments 200.00 PHP
LOAN 20,000.00 PHP
Monthly Installments 500.00 PHP
APPROVED IN 3 MINUTES
APP STORE
Install now
Sponsored
Anuman ang dapat gawin, pag-unlad sa buhay,
At upang makuha ang pakiramdam ng tagumpay,
Ang unang hakbang na iyon ay mahalaga.
Amount 5,000 Repayment 5,050
Amount 10,000 Repayment 10,100
Amount 15,000 Repayment 15,145
Amount 20,000 Repayment 20,190
No Service Fee
LOAN
APP STORE

Figure 36: Adverts on Phone.



Dear [redacted]--You have Rs.28,000 available in your account, withdraw now: https://bit.ly/[redacted]

[redacted]Your approved money is2.8 lahks! You need to complete credit check ASAP! It expires in 8 hours! Please complete ASAP! https://bit.ly/[redacted]

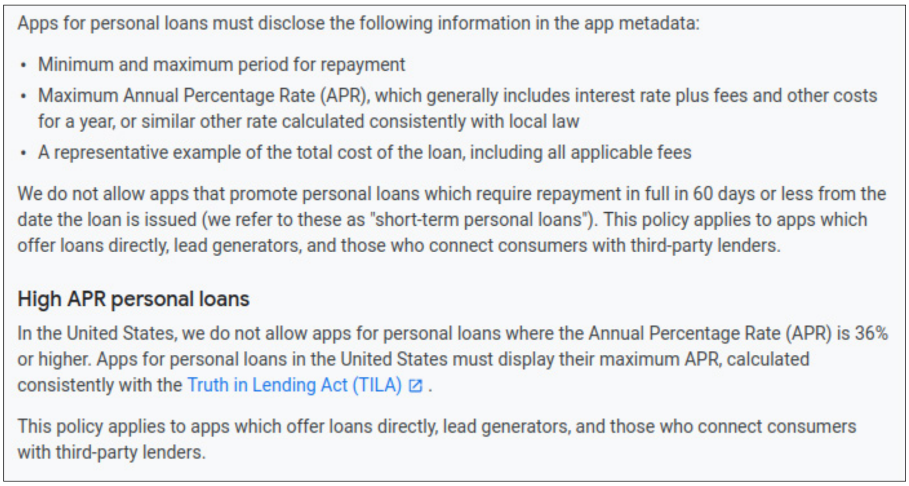
Figure 37: Loan app distribution SMS adverts.

VIOLATING AND CIRCUMVENTING APP PLATFORM POLICIES

Traditional malware tries to evade app reviewers by using anti-sandbox techniques, dropping the payload, decrypting code at runtime, and downloading code at a later stage of the malware. In the case of spyware personal loan apps, they access and exfiltrate user data by declaring it publicly on app platforms. The abuse of the data collected from the borrower's device happens outside the app platforms. We call these types of threats 'holistic threats'. If you do not have a complete sense of how, when, and where, including the context of the threat, the threat will not seem malicious.

In the early days of personal loan apps, especially in developing nations, these apps charged up to 200% [4], due to a lack of policies in countries such as Nigeria, Kenya and India. App stores were controlling the policies of these apps. The interest rates were high, the loan terms were short, and pretty much anyone could publish a loan app and lend to individuals.

The first policy we are aware of came in 2019, requiring apps to stop short-term loans of less than 60 days, specify additional metadata about the loan, such as interest rates and fees, and reduce the APR to 36% in the US – but there was no such requirement for the APR to be reduced in developing countries, where vulnerable users were most affected [10].



Apps for personal loans must disclose the following information in the app metadata:

- Minimum and maximum period for repayment
- Maximum Annual Percentage Rate (APR), which generally includes interest rate plus fees and other costs for a year, or similar other rate calculated consistently with local law
- A representative example of the total cost of the loan, including all applicable fees

We do not allow apps that promote personal loans which require repayment in full in 60 days or less from the date the loan is issued (we refer to these as "short-term personal loans"). This policy applies to apps which offer loans directly, lead generators, and those who connect consumers with third-party lenders.

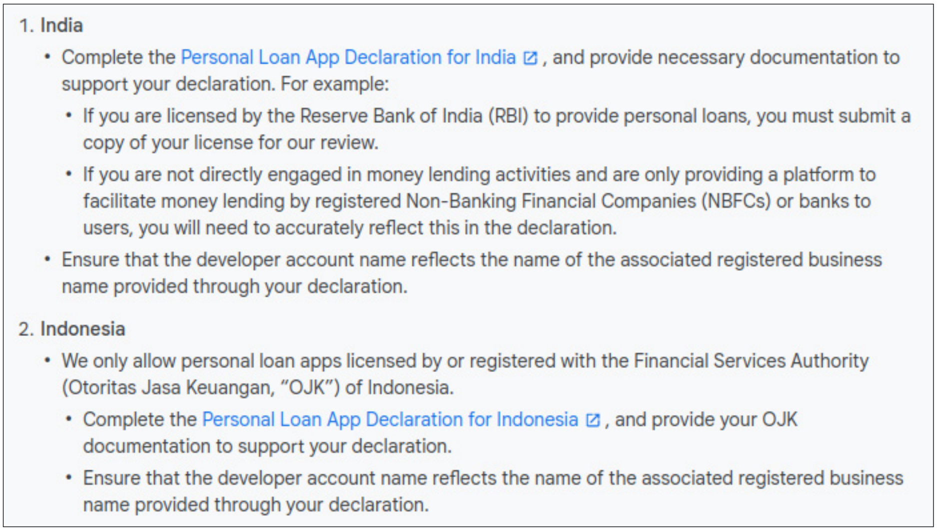
High APR personal loans

In the United States, we do not allow apps for personal loans where the Annual Percentage Rate (APR) is 36% or higher. Apps for personal loans in the United States must display their maximum APR, calculated consistently with the Truth in Lending Act (TILA) .

This policy applies to apps which offer loans directly, lead generators, and those who connect consumers with third-party lenders.

Figure 38: Google Play Store policy update in 2019.

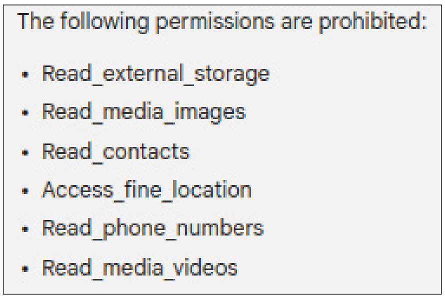
As more abusive loan apps started appearing, in September 2021 [11] the policy was updated to introduce the requirement (in India and Indonesia) to submit an app declaration, in which it was necessary, for example, to declare whether the app was licensed by a legitimate bank or associated with a central bank-approved finance company, and submit supporting documentation.



1. India
   - Complete the Personal Loan App Declaration for India , and provide necessary documentation to support your declaration. For example:
     - If you are licensed by the Reserve Bank of India (RBI) to provide personal loans, you must submit a copy of your license for our review.
     - If you are not directly engaged in money lending activities and are only providing a platform to facilitate money lending by registered Non-Banking Financial Companies (NBFCs) or banks to users, you will need to accurately reflect this in the declaration.
   - Ensure that the developer account name reflects the name of the associated registered business name provided through your declaration.
2. Indonesia
   - We only allow personal loan apps licensed by or registered with the Financial Services Authority (Otoritas Jasa Keuangan, "OJK") of Indonesia.
     - Complete the Personal Loan App Declaration for Indonesia , and provide your OJK documentation to support your declaration.
     - Ensure that the developer account name reflects the name of the associated registered business name provided through your declaration.

Figure 39: Google Play Store policy updates from 2021.

This policy now covers other countries including the Philippines, Nigeria, Kenya and Pakistan, with various requirements for personal apps to operate in those countries [12]. At the time of writing, the use of sensitive permissions that steal data has been prohibited [13].There is still a possibility the crooks could directly collect that data from the borrowers, though less data will be transferred.



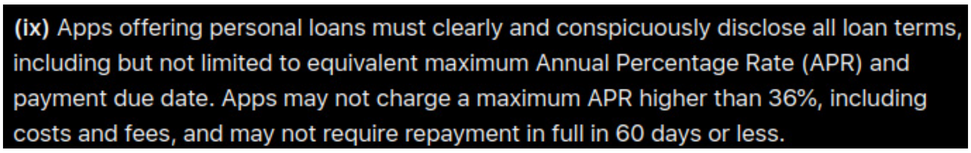
The following permissions are prohibited:

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos

Figure 40: Permissions prohibited from personal loan apps since 31 May 2023.

Several data-stealing personal apps have been removed [14] from the *Apple App Store*, but due to the popularity of *Android* in developing nations, they are more commonly found in the *Google Play Store*.

The personal loan policy for *Apple* [15] has some of the same requirements as the *Google Play Store* but doesn't have country-specific rules.

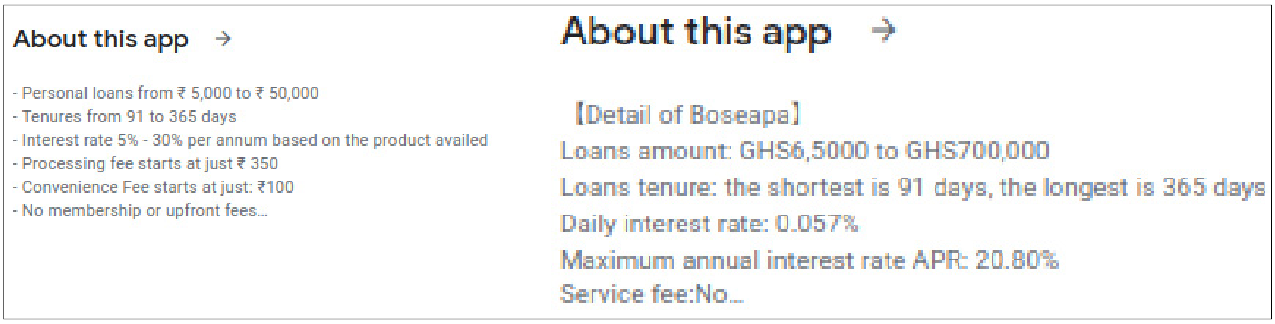


(ix) Apps offering personal loans must clearly and conspicuously disclose all loan terms, including but not limited to equivalent maximum Annual Percentage Rate (APR) and payment due date. Apps may not charge a maximum APR higher than 36%, including costs and fees, and may not require repayment in full in 60 days or less.

Figure 41: Apple App Store policy for personal loans.

Max APR and loan term violation

These apps include details of loan tenure, loan amount range, and interest rate information in their app descriptions. They claim to give borrowers at least 90 days for repayment. However, these details are included in the app description page merely to appear to comply with the policy. But whether or not the behaviour of the apps actually complies with the policy cannot be monitored by the app platforms. The recovery agents who have the data will start calling on the fifth, sixth or seventh day [16], or in the best case, after a couple of weeks, depending on the level of malicious intent. Store policy is only paid lip service.



About this app →

- Personal loans from ₹ 5,000 to ₹ 50,000
- Tenures from 91 to 365 days
- Interest rate 5% - 30% per annum based on the product availed
- Processing fee starts at just ₹ 350
- Convenience Fee starts at just: ₹100
- No membership or upfront fees...

About this app →

【Detail of Boseapa】
Loans amount: GHS6,5000 to GHS700,000
Loans tenure: the shortest is 91 days, the longest is 365 days
Daily interest rate: 0.057%
Maximum annual interest rate APR: 20.80%
Service fee:No...

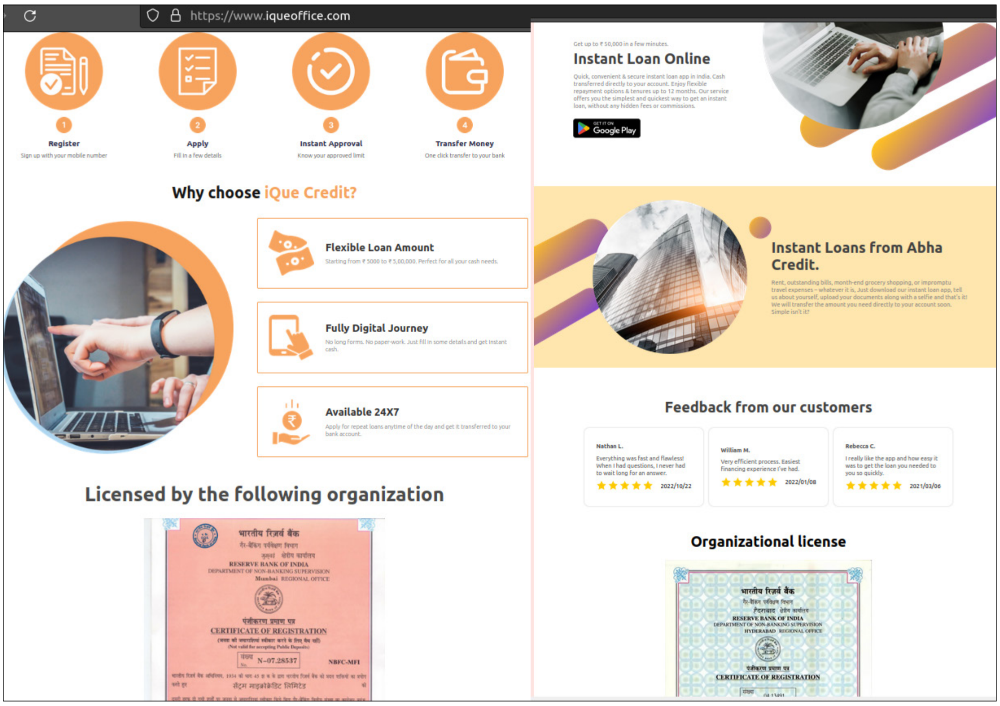
Figure 42: Loan description page.

NBFC and bank certificates

In most of the worst affected countries, one of the requirements for these apps to start lending is either to get a licence directly from the central bank or, if they claim to provide only the lending platform, to be associated with central bank-approved financial tech companies [12].

For instance, in India, fintech companies that do not have direct lending licences from the central bank, called the RBI, use NBFCs (non-banking financial companies), which are regulated by the central bank, for lending through mobile apps.

We checked some of the websites of spyware loan apps that were targeting Indian users. These websites had images of central bank issued NBFC certificates to convince users. We tried to contact some of them, but received no response. The Indian central bank has a list of approved NBFCs [17], and we found that the names exist on that list. It is likely that the spyware loan apps have used their certificates or, based on investigations by local authorities in the past, the loan apps piggybacked on the existing NBFCs and paid them commission – a practice which is considered illegal [13] [18].



https://www.iqueoffice.com

1 Register
Sign up with your mobile number

2 Apply
Fill in a few details

3 Instant Approval
Know your approved limit

4 Transfer Money
One click transfer to your bank

Why choose iQue Credit?

Flexible Loan Amount
Starting from ₹ 5000 to ₹ 5,00,000. Perfect for all your cash needs.

Fully Digital Journey
No long forms. No paper-work. Just fill in some details and get instant cash.

Available 24X7
Apply for repeat loans anytime of the day and get it transferred to your bank account.

Licensed by the following organization

भारतीय रिज़र्व बैंक
गैर-बैंकिंग पर्यवेक्षण विभाग
मुम्बई क्षेत्रीय कार्यालय
RESERVE BANK OF INDIA
DEPARTMENT OF NON-BANKING SUPERVISION
Mumbai REGIONAL OFFICE
पंजीकरण प्रमाण पत्र
CERTIFICATE OF REGISTRATION
(Not valid for accepting Public Deposits)
संख्या No. N-07.28537 NBFC-MFI
सैटम माइक्रोक्रेडिट लिमिटेड

Get up to ₹ 50,000 in a few minutes.

Instant Loan Online

Quick, convenient & secure instant loan app in India. Cash transferred directly to your account. Enjoy flexible repayment options & tenures up to 12 months. Our service offers you the simplest and quickest way to get an instant loan, without any hidden fees or commissions.

GET IT ON Google Play

Instant Loans from Abha Credit.

Rent, outstanding bills, month-end grocery shopping, or impromptu travel expenses – whatever it is, Just download our instant loan app, tell us about yourself, upload your documents along with a selfie and that's it! We will transfer the amount you need directly to your account soon. Simple isn't it?

Feedback from our customers

Nathan L.
Everything was fast and flawless! When I had questions, I never had to wait long for an answer.
★★★★★ 2022/10/22

William M.
Very efficient process. Easiest financing experience I've had.
★★★★★ 2022/01/08

Rebecca C.
I really like the app and how easy it was to get the loan you needed to you so quickly.
★★★★★ 2021/03/06

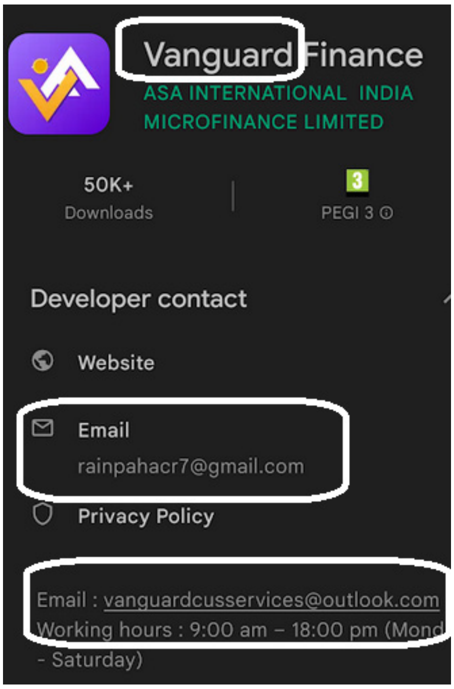
Organizational license

भारतीय रिज़र्व बैंक
गैर-बैंकिंग पर्यवेक्षण विभाग
हैदराबाद क्षेत्रीय कार्यालय
RESERVE BANK OF INDIA
DEPARTMENT OF NON-BANKING SUPERVISION
HYDERABAD REGIONAL OFFICE
पंजीकरण प्रमाण पत्र
CERTIFICATE OF REGISTRATION

Figure 43: RBI certificates used by loan apps with non-banking financial company (NBFC) name.

USE OF KNOWN BRANDS

Impersonating known brands is illegal. Lots of these apps use known names or brand names that are similar to known ones to attract users and make them seem legitimate. In Figure 44 you can see an app using the Vanguard brand name. Based on our investigation, the app doesn't look related to the legitimate brand, with a *Gmail* email address and an *Outlook* customer service address.



Vanguard Finance
ASA INTERNATIONAL INDIA MICROFINANCE LIMITED

50K+ Downloads | PEGI 3

Developer contact

Website

Email
rainpahacr7@gmail.com

Privacy Policy

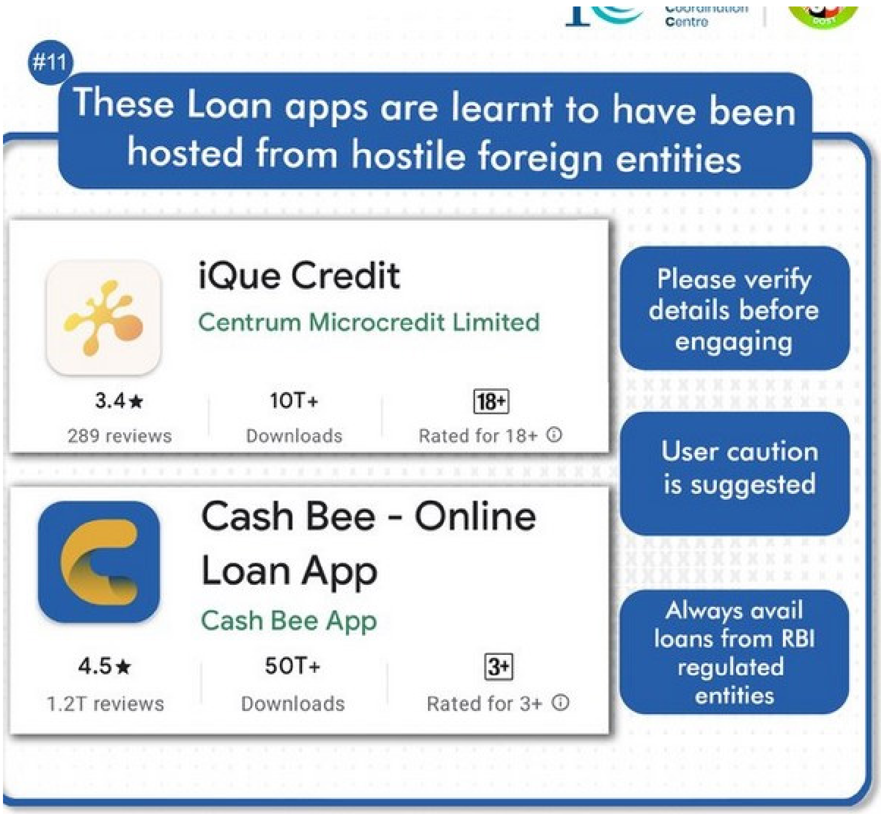
Email : vanguardcusservices@outlook.com
Working hours : 9:00 am – 18:00 pm (Mond
- Saturday)

Figure 44: App using well-known Vanguard brand.

DATA ESPIONAGE AND HOSTILITY

A simplified definition of espionage could be written as 'the practice of spying to obtain information'. These spyware loan apps do exactly that, using mobile devices and app platforms. They collect huge amounts of data, and though they specify this in the privacy policy, the real reason for which it has been used so far is different. Not everyone is aware of the dangers that collecting data could pose [3]. We do not know who else the data was shared with or how it will be used in the future.

We don't see any apps collecting this kind of data through app platforms, including the *Apple App Store*, other than those labelled as spyware. Here, the apps claiming to be loan apps were allowed to access sensitive data, without any bounds, especially during the early days.



Coordination Centre

#11

These Loan apps are learnt to have been hosted from hostile foreign entities

iQue Credit

Centrum Microcredit Limited

3.4★ 289 reviews | 10T+ Downloads | 18+ Rated for 18+ ⓘ

Cash Bee - Online Loan App

Cash Bee App

4.5★ 1.2T reviews | 50T+ Downloads | 3+ Rated for 3+ ⓘ

Please verify details before engaging

User caution is suggested

Always avail loans from RBI regulated entities

Figure 45: Indian cybercrime centre labelling spyware apps as hosted from hostile foreign entity.

India and China were at war in 1962, and since 2020 there have been several border disputes, several Chinese apps are banned in India, and anything hosted in China or data shared with China is considered hostile [19].

DEFUNCT FINANCE ORGANIZATIONS AND SHELL COMPANIES

The earliest documented evidence of extortionist spyware apps dates from 2016 in China [5]. Several Chinese students were offered high-interest loans through mobile apps with access to sensitive data. Students who failed to pay dues were threatened with sending out their nude photographs to the contacts.

During the pandemic and post-pandemic years, similar extortionist apps started to appear in different countries across Asia and Africa, abusing the access of app store platforms to these countries.

Authorities in some countries, like India, have cracked down on these apps, apprehended several local culprits, and released the working and organizational chart behind these rackets [5, 20].

Based on that information, the kingpins behind these operations are thought to be Asian-based and located across different Asian countries. They begin by advertising on local recruitment websites for directors and use them as fronts to run operations. They tried to get a lending licence, but were rejected by the central banks, so they used joint collaboration with NBFCs, which are allowed to lend with banking licences. They use the local directors hired in the previous stage to sign up defunct NBFCs, and the defunct NBFCs get commission for their part. They open bank accounts using those NBFCs and create shell companies to transfer money. After this, they recruit local unemployed people as calling staff to make extortion calls and, for lower salaries, as image and video editors to doctor the images. They are given access to borrower data exfiltrated through the apps. The communications between the kingpins and locals are through apps like *WeChat* and *GBWhatsApp* (a modified version of *WhatsApp*) [20].

The money recovered from the borrowers after expenses is then sent through different bank accounts registered under different shell companies before reaching the final account, where it is converted to cryptocurrency and sent to the kingpins. Because the kingpins are located in a different country and lack jurisdiction, they are never apprehended.

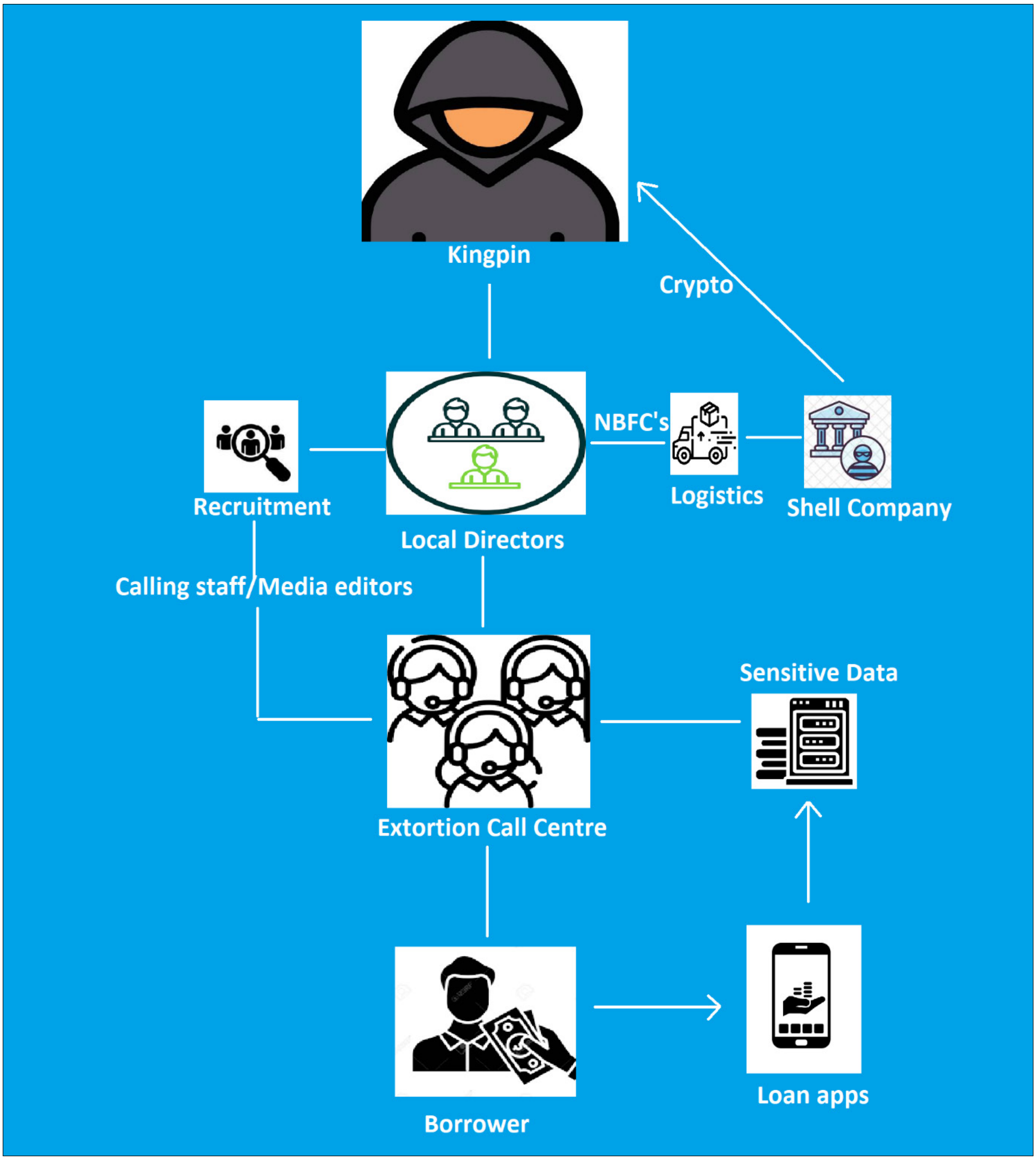


Figure 46: Organization and workflow chart of spyware loan apps.

WHY MEGA -LO-(AN)-DON?

Megalodon is an extinct species of shark that is thought to be the biggest shark ever to have lived [21]. Traditional terms associated with unfair lending, such as loan sharks and predatory lending, are not sufficient for these apps. These are, in most cases, illegal, unfair and abusive, use threats, and have taken innocent lives. Besides that, we believe these are run by organized groups that have spread their wings across borders to target vulnerable people.

Mega-Loan-Don is probably the most appropriate term to describe the monstrosity, scale of reach, unfair terms, abusive tactics, and mode of operation of these apps.

CONCLUSION

Mobile fintech and app platforms have revolutionized the way things work for ordinary users with digital banking, trading, and access to countless things that they didn't have access to before, especially in the developing world where mobile is the only way to access the internet [22]. App stores like the *Apple App Store* and *Google Play Store* make it possible for any innovation around the world to reach billions of mobile users. This kind of access and reach comes with its own risks. Because mobile is a personal device, a lot of personal data from day-to-day life is stored, and storing this data has its own risks. The combination of both of these risks is very dangerous. Instant personal loans by Megalo(an)don apps are one such threat that has been expertly exploited under the guise of a finance app.

What started in China [23] has spread all over the developing world, targeting those shunned by traditional banks, usually the bottom of society, and those who are after immediate, short-term loans. Local government had not anticipated these mobile threats, and there have been hardly any policies to curb them, resulting in malicious apps colluding with local crooks to disburse loans at quick rates with high interest rates and fees, and using the sensitive data access provided by the mobile device to make threatening calls to those who were unable to repay, tragically even leading to several suicides due to the inability of the victim to bear the shame of the spreading of doctored images and videos.

To prevent abuse of this kind in the future, governments should bring in laws to stop abuse of the app store platform from being used to target their citizens. Banning these apps completely is not a solution, we think producing a whitelist of legal apps, coordinating with *Apple* and *Google* to effectively implement a way for lawful apps to provide service to citizens, will help curb this threat.

ACKNOWLEDGEMENTS

Spyware loan apps have been a problem for years. Several industry colleagues and mobile security researchers have been raising concern about this for some time and bringing it to the app platforms' attention. Because of their efforts, there have been several policies, and thousands of apps have been removed. Thanks to everyone for working on this issue. Kudos to the @malwarehunterteam for being an early advocate on this, and thanks to Nirav Parekh for reporting some of the apps.

REFERENCES

[1] AppsFlyer. How mobile apps are transforming finance in Africa. https://www.appsflyer.com/infograms/africa-google-trends-report-11-2022/.

[2] Google. Play Console Help. https://support.google.com/googleplay/android-developer/answer/9876821.

[3] Collins, W. M.; Yasemin, A.; Adam, J. A. Desperate Times Call for Desperate Measures: User Concerns with Mobile Loan Apps in Kenya. 2022 IEEE Symposium on Security and Privacy.

[4] Whitwam, R. Google Ban Fails to Stamp Out Short-Term Payday Lending Apps. Android Police. 21 August 2019. https://www.androidpolice.com/2019/08/21/google-publishes-play-store-policies-for-personal-loan-apps/.

[5] Kannan, S. How China-based money lending apps are devastating gullible Indian borrowers. India Today. January 2021. https://www.indiatoday.in/india/story/deep-dive-how-china-based-money-lending-apps-devastating-gullible-indian-borrowers-1756569-2021-01-06.

[6] Bansal, V. Shame, suicide and the dodgy loan apps plaguing Google's Play Store. Wired UK. 20 January 2021. https://www.wired.co.uk/article/google-loan-apps-india-deaths.

[7] Singh, J. Predatory loan apps in India rake in huge fees, and are driving some users to suicide. Tech Crunch. 26 August 2022. https://techcrunch.com/2022/08/26/loan-apps-abuse-harassment-suicide-indian-users-google-apple-india/.

[8] Ortega, F. Predatory Loan Scam Campaigns Move to Flutter. Zimperium. 15 December 2022. https://www.zimperium.com/blog/moneymonger-predatory-loan-scam-campaigns-move-to-flutter/#.

[9] Urgentt Loan with Calculator app. https://play.google.com/store/apps/details?id=com.finance.loanadvisorpesso.emicalculator.

[10] Milder, Z.; Faux, Z. Google Ban Fails to Stamp Out Short-Term Payday Lending Apps. Bloomberg. 24 January 2020. https://www.bloomberg.com/news/articles/2020-01-24/google-ban-fails-to-stamp-out-short-term-payday-lending-apps.

[11] Google. Play Console Help. https://web.archive.org/web/20210926053140/https://support.google.com/googleplay/android-developer/answer/9876821.

[12] Google. Play Console Help. https://web.archive.org/web/20230427153814/https://support.google.com/googleplay/android-developer/answer/9876821.

[13] Google. Play Console Help. https://support.google.com/googleplay/android-developer/answer/13161491.

[14] Xiong, R.; Dasgupta, R.; Mambo, A. Lookout Discovers Hundreds of Predatory Loan Apps on Google Play and Apple App Store. Lookout. 30 November 2022. https://www.lookout.com/blog/predatory-loan-apps.

[15] Apple. App Store Review Guidelines. https://developer.apple.com/app-store/review/guidelines/.

[16] Loan apps threat from Indonesia. November 2022. https://mediakonsumen.com/2022/11/05/surat-pembaca/dc-pinjol-yang-mengancam-akan-melakukan-penggalangan-dana.

[17] Reserve Bank of India. NBFC approved list. https://www.rbi.org.in/Scripts/BS_NBFCList.aspx.

[18] The Times of India. ED attaches funds of NBFC in loan apps probe case. 12 January 2022. https://timesofindia.indiatimes.com/business/india-business/ed-attaches-funds-of-nbfc-in-chinese-funded-instant-loan-apps-probe-case/articleshow/88860949.cms.

[19] BBC News. India-China dispute: The border row explained in 400 words. 14 December 2022. https://www.bbc.co.uk/news/world-asia-53062484.

[20] Sharma, A. Illegal Lending Apps Rely on A Tangle of Shell Companies, Cryptocurrency to Lie Low. News 18. 3 October 2022. https://www.news18.com/news/india/loan-wolves-of-china-illegal-lending-apps-rely-on-a-tangle-of-shell-companies-cryptocurrency-to-lie-low-5809513.html.

[21] Davis, J. Megalodon: the truth about the largest shark that ever lived. Natural History Museum. https://www.nhm.ac.uk/discover/megalodon--the-truth-about-the-largest-shark-that-ever-lived.html.

[22] Silver, L.; Smith, A.; Johnson, C.; Jiang, J.; Anderson, M.; Rainie, L. Mobile connectivity in emerging economies. Pew Research Center. 7 March 2019. https://www.pewresearch.org/internet/2019/03/07/mobile-connectivity-in-emerging-economies/.

[23] The Times of India. How instant loan apps drained crores from borrowers. https://timesofindia.indiatimes.com/business/india-business/how-instant-loan-apps-drained-crores-from-borrowers/articleshow/80170284.cms.

[24] Chadha, S. Loan apps: How to protect yourself from such scams. The Times of India. May 2022. https://timesofindia.indiatimes.com/business/india-business/loan-apps-how-to-protect-yourself-from-such-scams/articleshow/91487086.cms.