Research Report on:
‘Pradhan Mantri Yojana Loan’ Scheme

Analysed objects: a) Pradhan Mantri Yojana Loan app
b) https://www.pradhanmantriyojanaloan[.]com website.
DISCALIMER

This report is purely based on technical findings made by the research team during the investigation. It is not intended to malign or in any way target any country, actor or person through the findings. All the information provided in the report has been extracted during the investigation.
The Research Wing of CyberPeace Foundation has found an android application available on the Google play store having the name of ‘Pradhan Mantri Yojana Loan’.
App Analysis:

The Research Wing at CyberPeace Foundation along with the Research wing of Autobot Infosec Private Limited started an in-depth investigation on the application to come to a conclusion whether the app has actually been launched by Govt. of India or it is an online fraud.

Application Details:

<table>
<thead>
<tr>
<th>App name</th>
<th>Pradhan Mantri Yojana Loan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package name</td>
<td>com.pm.pmloanyoujna</td>
</tr>
<tr>
<td>Average CVSS Score</td>
<td>6.4</td>
</tr>
<tr>
<td>App Security Score</td>
<td>35%</td>
</tr>
<tr>
<td>Main Activity</td>
<td>com.pm.pmloanyoujna.activitySplashActivity</td>
</tr>
<tr>
<td>Target SDK</td>
<td>30</td>
</tr>
</tbody>
</table>
App components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activities</td>
<td>17</td>
</tr>
<tr>
<td>Services</td>
<td>1</td>
</tr>
<tr>
<td>Receivers</td>
<td>0</td>
</tr>
<tr>
<td>Providers</td>
<td>1</td>
</tr>
<tr>
<td>Exported Activities</td>
<td>0</td>
</tr>
<tr>
<td>Exported Services and Receivers</td>
<td>0</td>
</tr>
</tbody>
</table>

Application Certificate Details:

<table>
<thead>
<tr>
<th>Details</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>State</td>
<td>California</td>
</tr>
<tr>
<td>City</td>
<td>Mountain view</td>
</tr>
<tr>
<td>Organisation</td>
<td>Google</td>
</tr>
</tbody>
</table>

Application Permissions Details:

```xml
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="com.google.android.provider"/>
<uses-permission android:name="com.google.android.gms.permission.READ_CONTENT_PROVIDER"/>
<uses-permission android:name="android.permission.CAMERA"/>
```
<table>
<thead>
<tr>
<th>Permission</th>
<th>Status</th>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>android.permission.INTERNET</td>
<td>Normal</td>
<td>full Internet access</td>
<td>Allows an application to create network sockets.</td>
</tr>
<tr>
<td>android.permission.ACCESS_NETWORK_STATE</td>
<td>Normal</td>
<td>View network status</td>
<td>Allows an application to view the status of all networks.</td>
</tr>
<tr>
<td>android.permission.ACCESS_WIFI_STATE</td>
<td>Normal</td>
<td>View WI-FI Status</td>
<td>Allows an application to view the information about the status of Wi-Fi.</td>
</tr>
<tr>
<td>android.permission.WRITE_EXTERNAL_STORAGE</td>
<td>Dangerous</td>
<td>read/modify/delete external storage contents</td>
<td>Allows an application to write to external storage.</td>
</tr>
<tr>
<td>android.permission.READ_EXTERNAL_STORAGE</td>
<td>Dangerous</td>
<td>read external storage contents</td>
<td>Allows an application to read from external storage.</td>
</tr>
<tr>
<td>android.permission.CALL_PHONE</td>
<td>Dangerous</td>
<td>Directly call numbers</td>
<td>Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected behaviors.</td>
</tr>
<tr>
<td>Permission</td>
<td>Status</td>
<td>Information</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>android.permission.WAKE_LOCK</td>
<td>Normal</td>
<td>prevent phone from sleeping</td>
<td>Allows an application to prevent the phone from going to sleep.</td>
</tr>
<tr>
<td>android.permission.CAMERA</td>
<td>Dangerous</td>
<td>Take pictures and videos</td>
<td>Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.</td>
</tr>
<tr>
<td>com.google.android.gm.permission.READ_CONTENT_PROVIDER</td>
<td>Unknown</td>
<td>Unknown permissions</td>
<td>Unknown permission from android reference</td>
</tr>
</tbody>
</table>

1. Clear Traffic is enabled by App (Risk is medium)

```xml
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
  <base-config cleartextTrafficPermitted="true">
    <trust-anchors>
      <certificates src="system"/>
    </trust-anchors>
  </base-config>
</network-security-config>
```
2. Activity is not Protected and an intent-filter exists. An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported. There is a possibility of a backdoor like service present.

**Domains used by App**

1. **stripe.com**  
   IP: 54.187.159.182  
   Country: United States of America  
   Region: Oregon  
   City: Portland  
   Latitude: 45.523449  
   Longitude: -122.676208

2. **educationtak.com**  
   IP: 162.144.109.102  
   Country: United States of America  
   Region: Utah  
   City: Provo  
   Latitude: 40.213909  
   Longitude: -111.634071  
   Under, this head Research Team’s feedback as per past records of the site was found dangerous for its users.

3. **www.pradhanmantriyojanaloan[.]com** (Domain name having the similar name with the App.)  
   IP: 111.118.215.174  
   Country: India  
   Region: Delhi  
   City: Delhi  
   Latitude: 28.66667  
   Longitude: 77.216667  
   Again under this website the IP has the past records for phishing attacks and malicious activity.

4. **wa.me**  
   IP: 69.171.250.60  
   Country: Netherlands  
   Region: Noord-Holland  
   City: Amsterdam  
   Latitude: 52.374031  
   Longitude: 4.88969
Email Address Associated

a. rishi@domain.com [Extracted from the developer’s contact section]
b. support@stripe.com

```java
String str, String str2) throws InvalidRequestException {
    s, str2), urlEncode(str));
    to encode parameters to UTF-8. Please contact support@stripe.com for assistance.
    Exception e) {
        UnsupportedEncodingException {
            ConnectionRequest(requestMethod, str, createQuery, requestOptions);
            Exception e) {
                Property("com.google.appengine.runtime.environment", null) != null) {
                    eAppRequest(requestMethod, str, createQuery, requestOptions);

                codingException e2) {
                    requestException("Unable to encode parameters to UTF-8. Please contact support@stripe.com
```
## Email Analysis:

<table>
<thead>
<tr>
<th>Email ID</th>
<th>Exist?</th>
</tr>
</thead>
<tbody>
<tr>
<td>rishi********@gmail.com</td>
<td>Yes</td>
</tr>
</tbody>
</table>

As Google accepts the email id that means the email id does exist.

### SMTP session

```
[Contacting gmail-smtp-in.l.google.com [173.194.201.27]...]
[Connected]
220 mx.google.com ESMTP z15si7262578oid.91 - gsmtp
EHLO mx1.
250-mx.google.com at your service, [75.126.251.247]
250-SIZE 1572086400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250-SMTPUTF8
MAIL FROM:<>
250 2.1.0 OK z15si7262578oid.91 - gsmtp
RCPT TO:<rishi********@gmail.com>
250 2.1.5 OK z15si7262578oid.91 - gsmtp
RSET
250 2.1.5 Flushed z15si7262578oid.91 - gsmtp
QUIT
[Connection closed]
```
Some information has been extracted by Open Source Intelligence techniques.

<table>
<thead>
<tr>
<th>Email</th>
<th>rishi********@gmail.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google ID</td>
<td>116406814636176809272</td>
</tr>
<tr>
<td>Last Update</td>
<td>2021-01-01 23:42:52</td>
</tr>
</tbody>
</table>

```json
{
  "results": [
    {
      "suggestion": "rishi********@gmail.com",
      "objectType": "PERSON",
      "person": {
        "personId": "116406814636176809272",
        "metadata": {
          "ownerId": "116406814636176809272",
          "objectType": "PERSON"
        }
      }
    }
  ]
}
```

personId is the Google ID of the mentioned email id
i.e 116406814636176809272

As of now the time of the report is being written, no social profile has been found on any reputed platform linked with this email id.

<table>
<thead>
<tr>
<th>Social Platform</th>
<th>Account Existence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>No</td>
</tr>
<tr>
<td>Twitter</td>
<td>No</td>
</tr>
<tr>
<td>Instagram</td>
<td>No</td>
</tr>
<tr>
<td>Linkedin</td>
<td>No</td>
</tr>
</tbody>
</table>

We have not observed this email address on major services like LinkedIn, Facebook, or other sources. A lack of digital presence may simply indicate a new email address, but is typically suspicious.
Support@stripe.com

Striper is a reputable payment receiving infrastructure for business and enterprise. This email address is available in 14 reputable sources on the internet, and has profiles on well-known sites like Twitter and Gravatar.

Analysis on www.pradhanmantriyojanaloan.com:

As we found the app is linked with a domain that has a similar name with the app itself, we proceed the investigation further on the website.

### AIMS OF PRADHAN MANTRI JAN AWAS YOJANA

Providing houses to poor families of the state, who have no accommodation to live with. Through this scheme, they will be given 2 BHK flats, which are not worth the price (Rs 1000 per square feet).

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Type of Family</th>
<th>Area (sq ft)</th>
<th>No. of Rooms</th>
<th>Rent (Rs)</th>
<th>Land (sq ft)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EWS</td>
<td>120,000</td>
<td>2</td>
<td>325.70</td>
<td>3,908,400</td>
</tr>
<tr>
<td>2</td>
<td>LIG</td>
<td>120,000</td>
<td>2</td>
<td>505.25</td>
<td>6,003,000</td>
</tr>
</tbody>
</table>

### PRADHAN MANTRI AWAS YOJANA FACILITIES

- [Image](https://www.pradhanmantriyojanaloan.com/facilities.php)
On the page https://www.pradhanmantriyojanaloan[.]com/emitra-registration.php
A registration form for emitra can be seen which asks personal information like Name, Emitra code, Mobile, State, City as well as the bank account details like A/c Name, IFSC code, A/c No. Branch Name.

Image: https://www.pradhanmantriyojanaloan[.]com/emitra-registration.php

After providing some randomly chosen dummy data it redirects to the https://www.pradhanmantriyojanaloan[.]com/common-thanks.php with a Thank You message.

Image: https://www.pradhanmantriyojanaloan[.]com/common-thanks.php
In Depth Investigation:

Some key findings extracted during the investigation are mentioned below:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>pradhanmantriyojanaloan[].com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>111.118.215.174</td>
</tr>
<tr>
<td>Hostname</td>
<td>bh-in-19.webhostbox.net</td>
</tr>
<tr>
<td>Organisation</td>
<td>Hostgator GPX India</td>
</tr>
<tr>
<td>ISP</td>
<td>PDR</td>
</tr>
<tr>
<td>ASN</td>
<td>394695</td>
</tr>
<tr>
<td>Country</td>
<td>India</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Registry Domain ID: 2472484582_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2020-12-28T05:08:14Z
Creation Date: 2019-12-27T09:32:34Z
Registry Expiry Date: 2021-12-27T09:32:34Z

Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952

Registrant Name: Sanjeev Sharma*
Registrant Street: 26/293, Civil Lines, Near gopal cinema, Alwar
Registrant City: Alwar
Registrant State/Province: Rajasthan
Registrant Postal Code: 301001
Registrant Country: IN (India)
Registrant Phone: +91.941401
Registrant Email: solutions.compuses@gmail.com

Name Server: ns1.bh-in-19.webhostbox.net
            ns2.bh-in-19.webhostbox.net
Doing some Open source investigation on the **Registrant Email** id we got to know that the email id has been used to register for many websites. Some of those websites have the **Registrant Name** as Vivek, **Registrant Organization** as COMPUSYS, **Registrant State/Province** as Rajasthan with the same **Registrant Email** as solutions.compusys@gmail.com. After that we moved forward the open source investigation with the combination of the three key values ‘Vivek’, ‘COMPUSYS’ and ‘Rajasthan’ and got a common result i.e **Compusys E Solutions** which is a ‘WEB DESIGN DEVELOPMENT COMPANY IN JAIPUR’.

**Image**: Home Page https://www.compusyessolutions.com/

<table>
<thead>
<tr>
<th><strong>Company Name</strong></th>
<th><strong>Compusys e Solutions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contact Number</strong></td>
<td>+91 9460 36 (redacted)</td>
</tr>
<tr>
<td><strong>Skype id</strong></td>
<td>vivekces</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>47/195, Rajat Path, New Sanganer Road, Mansarover, Jaipur - 302020, Rajasthan - INDIA</td>
</tr>
<tr>
<td><strong>CIN</strong></td>
<td>U72900RJ2015PTC048841</td>
</tr>
<tr>
<td><strong>Website</strong></td>
<td><a href="https://www.compusyessolutions.com/">https://www.compusyessolutions.com/</a></td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>111.118.215.174</td>
</tr>
</tbody>
</table>

It can be seen that both the websites pradhanmantriyojanaaloan[]com and https://www.compusyessolutions.com/ are hosted on the same IP address i.e 111.118.215.174.

On the page https://www.pradhanmantriyojanaaloan[]com/pradhanmantri-awas-yojana-gramin.php a link of http://www.pmawasyojana[]in website is given to describe the feature of **Pradhan Mantri Awas Yojana (PMAY)** instead of giving the official PMAY website i.e https://pmaymis.gov.in/.
On the page --

https://www.pradhanmantriyojanaaloan[][].com/pradhanmantri-bhukhand-nirman-yojana.php --

The website of the Common Service Centres (CSC) and Pradhan Mantri Awas Yojana are mentioned as pradhanmantriyojanaaloan[][].com instead of mentioning the official website https://www.csc.gov.in/ and https://pmaymis.gov.in/ respectively.
After clicking the orange Apply Loan button from the nav bar it redirects user to https://www.pradhanmantriyojanaloan[].com/apply-loan.php page which asks for a number of personal information like First Name, Middle Name, Last Name, Gender, Date of Birth, Husband Name/Wife Name, Father’s name, Mother’s name, Mobile, State, City, Pincode, loan amount, Aadhar Card number, bank account details like A/c Name, IFSC Code, A/c No, Branch Name etc. Also it asks users to upload their passport size image, Ration Card and an address proof.

Image: https://www.pradhanmantriyojanaloan[].com/apply-loan.php

We noticed the acceptable size of the image mentioned here is 175*175 but we uploaded a dummy image with a larger size and it was successfully uploaded. As we all know that Aadhar is a 12 digits unique number but during our investigation in the field of Aadhar Card a random number larger than 12 digits was entered and it had been successfully processed.

After clicking the Submit button it takes the user to a page https://www.pradhanmantriyojanaloan[].com/thank-you.php asking for OTP sent to the mobile number given during the application for loan. While investigation we didn't receive any OTP.

Also at the bottom of the page it shows the details that have been submitted during the application.
We have been assigned with a 10 digit receipt number. Which was then used on the https://www.pradhanmantriyojanaloan[.]com/check-status.php page.
Initially it was assumed that the receipt number would not work as we could not submit the OTP but it was accepted and the status was shown as ‘Your Application is Submitted. Thank you!’.
On the Contact Us page there is an image having the symbol of the Government of India. Hence, the site is pretending to be a Government of India entity and it was observed that there are grammatical and spelling mistakes on the image.

Also the image consists of a QR code.
After decoding the QR code we got a PhonePe not a Merchant UPI string --

```
upi://pay?pa=Q95811869@ybl&pn=PhonePeMerchant&mc=0000&mode=02&purpose=00&orgid=180001&sign=MEUClQCAVhdpMMhrrPhefrf8EZ0cgIzPWXxUeGj/+IR4kkQzWqglGvWv2y0wJU/TjVY2eaAZbaii39HoDK4Zhcgio6VEyQ0w=
```

We tried to verify the UPI id Q95811869@ybl but we concluded with an invalid UPI id message.

In source code analysis we found some information like --

- The title of the site is 'Pradhanmantri Yojana Loan'

- The title image has the symbol of Government of India
  [https://www.pradhanmantriyojanaloan[.]com/images/favicon.png](https://www.pradhanmantriyojanaloan[.]com/images/favicon.png)

- There is a string //echo "DESKTOP"; in the navbar. It changes depending on the user's device i.e user agent like //echo "TABLET"; etc. It seems that the developer wanted to comment this section but mistakenly used // instead of <!-- --> which is a universal comment operator for HTML and not supposed to be shown on the website frontend layout. Showing this kind of unnecessary thing is bad practise of coding.

- From the source code two mobile numbers have been extracted +91-988762**** and +91-998276****. From open investigation on both the mobile numbers we got some information --

<table>
<thead>
<tr>
<th>MOBILE PHONE</th>
<th>988762****</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIRCLE CAPITAL</td>
<td>Jaipur</td>
</tr>
<tr>
<td>TELECOMS CIRCLE / STATE</td>
<td>Rajasthan</td>
</tr>
<tr>
<td>NETWORK</td>
<td>IDEA</td>
</tr>
<tr>
<td>SERVICE TYPE / SIGNAL</td>
<td>GSM</td>
</tr>
<tr>
<td>CONNECTION STATUS</td>
<td>LIVE - Active</td>
</tr>
</tbody>
</table>
We found there is an account linked with this number on Facebook.

+91-998276

| MOBILE PHONE       | 998276
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CIRCLE CAPITAL</td>
<td>Jaipur</td>
</tr>
<tr>
<td>TELECOMS CIRCLE / STATE</td>
<td>Rajasthan</td>
</tr>
<tr>
<td>NETWORK</td>
<td>VODAFONE</td>
</tr>
<tr>
<td>SERVICE TYPE / SIGNAL</td>
<td>GSM</td>
</tr>
<tr>
<td>CONNECTION STATUS</td>
<td>LIVE - Active</td>
</tr>
</tbody>
</table>
- Extracted email id -- info@pradhanmantriyojanaloan.com
The mail exchanger record (MX) has been found but the email id actually does not exist.

SMTP session
[Resolving mail.pradhanmantriyojanaloan.com...]
[Connected]
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO
250-bh-in-19.webhostbox.net Hello
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
MAIL FROM:<info@pradhanmantriyojanaloan.com>
RCPT TO:<info@pradhanmantriyojanaloan.com>
550 No Such User Here
Address has been rejected
QUIT
221 bh-in-19.webhostbox.net closing connection
[Connection closed]

- Extracted GST number -- 08A0HTV6905N1Z5.

We have tried to verify whether the gst number is valid or not on the https://services.gst.gov.in/ website. But it showed an invalid GSTIN message.
GSTIN consists of a 15 digit unique number having the state code and PAN information. The first two digits represent the state code, next 10 digits number is the PAN number of the entity. In this case state code 08 is representing Rajasthan.
We have also tried to verify the PAN number extracted from the given GSTIN but this again is ending with an invalid PAN number message.

The Website has directory listing enabled. Means anyone can visit the directory of the website and can borrow all the files, data from the directory.
Some of the directories contain a number of valuable files like **Aadhar card, PAN card, Ration Card, passport size photo** etc of peoples. Actually the directory contains the files that were uploaded through the **Apply Loan portal**. To verify and confirm this case, we checked with the files that have been uploaded from our end and got those files on the web directory.

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15935696</td>
<td>2020-07-01 02:12</td>
<td>3.0K</td>
<td></td>
</tr>
<tr>
<td>15935817</td>
<td>2020-07-01 05:36</td>
<td>8.1K</td>
<td></td>
</tr>
<tr>
<td>15935872</td>
<td>2020-07-01 07:09</td>
<td>2.6K</td>
<td></td>
</tr>
<tr>
<td>15935891</td>
<td>2020-07-01 07:39</td>
<td>8.3K</td>
<td></td>
</tr>
<tr>
<td>15935893</td>
<td>2020-07-01 07:41</td>
<td>8.3K</td>
<td></td>
</tr>
<tr>
<td>15935911</td>
<td>2020-07-01 08:12</td>
<td>5.2K</td>
<td></td>
</tr>
<tr>
<td>15936071</td>
<td>2020-07-01 12:39</td>
<td>6.9K</td>
<td></td>
</tr>
<tr>
<td>15936220</td>
<td>2020-07-01 16:46</td>
<td>7.5K</td>
<td></td>
</tr>
<tr>
<td>15937164</td>
<td>2020-07-02 19:00</td>
<td>3.6K</td>
<td></td>
</tr>
<tr>
<td>15937592</td>
<td>2020-07-03 06:54</td>
<td>6.1K</td>
<td></td>
</tr>
<tr>
<td>15937671</td>
<td>2020-07-03 09:05</td>
<td>4.3K</td>
<td></td>
</tr>
<tr>
<td>15937807</td>
<td>2020-07-03 12:51</td>
<td>5.1K</td>
<td></td>
</tr>
<tr>
<td>15940807</td>
<td>2020-07-07 00:12</td>
<td>8.9K</td>
<td></td>
</tr>
<tr>
<td>15942896</td>
<td>2020-07-09 10:14</td>
<td>6.7K</td>
<td></td>
</tr>
<tr>
<td>15942898</td>
<td>2020-07-09 10:16</td>
<td>6.7K</td>
<td></td>
</tr>
<tr>
<td>15946536</td>
<td>2020-07-13 15:23</td>
<td>4.8K</td>
<td></td>
</tr>
<tr>
<td>15946538</td>
<td>2020-07-13 15:23</td>
<td>4.8K</td>
<td></td>
</tr>
<tr>
<td>15946544</td>
<td>2020-07-13 15:33</td>
<td>4.8K</td>
<td></td>
</tr>
<tr>
<td>15946930</td>
<td>2020-07-14 02:17</td>
<td>6.6K</td>
<td></td>
</tr>
<tr>
<td>15946934</td>
<td>2020-07-14 02:24</td>
<td>6.6K</td>
<td></td>
</tr>
<tr>
<td>15947355</td>
<td>2020-07-14 11:11</td>
<td>8.8K</td>
<td></td>
</tr>
<tr>
<td>15948108</td>
<td>2020-07-15 11:01</td>
<td>5.3K</td>
<td></td>
</tr>
<tr>
<td>15949091</td>
<td>2020-07-16 14:19</td>
<td>4.8K</td>
<td></td>
</tr>
</tbody>
</table>

**Image**: Directory contains confidential files of the applicants
Here we see a spelling variation against the name of the scheme mentioned on the website i.e 'Pradhan Mantri Yojana Loan' and the main logo affixed on the website.

Image: Different spelling in the logo

Some of the images found on the web directory borrowed from stock photography. Some of the images actually have not been used on the website.

Image: Stock Images
By traversing the web directory we found a PhonePe merchant QR code. And after decoding it we got a string:

```
UPI: //pay?pa=02340122@ybl&pn=PhonePeMerchant&mc=0000&mode=02&purpose=00&orgid=180001&sign=MEUCIBsiL6JHImgc0RRuMXfPAnjnTkm4Z9tyJAhfq86txUcAiEAlj/Szlkxp1SidbXnWwdzu6JapU0w5l926cQ7q6qi5Ug8=
```

For this QR code we have also tried to verify but again got Invalid UPI id message.

During the investigation two admin login panels have been found:

- [https://www.pradhanmantriyojanaloan[]]com/admin/  
  ![Image](https://www.pradhanmantriyojanaloan[]]com/admin)

- [https://www.pradhanmantriyojanaloan[]]com/app_admin/  
  ![Image](https://www.pradhanmantriyojanaloan[]]com/app_admin)
We got a Privacy policy page (https://www.pradhanmantriyojanaloan[.]com/app_admin/privacy-policy.php) on the website which provides some description of the Loan App. We found the email id mentioned above rishi********@gmail.com on this page also.

Changes to This Privacy Policy
I may update our Privacy Policy from time to time. Thus, you are advised to review this page periodically for any changes. I will notify you of any changes by posting the new Privacy Policy on this page.
This policy is effective as of 2020-09-03

Contact Us
If you have any questions or suggestions about my Privacy Policy, do not hesitate to contact me at rishi********@gmail.com.

This privacy policy page was created at privacypolicytemplate.net and modified/generated by App Privacy Policy Generator

Image: https://www.pradhanmantriyojanaloan[.]com/app_admin/privacy-policy.php

- The copyright section in the footer section shows the year of copyright 2019.
Conclusive Summary:

1. The website has a domain of .com but usually any websites which belong to Government of India hosted on .gov.in or .nic.in.

2. There are many Grammatical mistakes in the website but usually Government websites do not make any Grammatical errors.

3. Personal details asked from the applicants i.e like Aadhar card, Ration card, PAN card are openly available on the website which can be misused by any Cyber criminal.

4. We have noticed some negligence on the code of the website like mentioned above, usually websites from any reputed entity do not have that kind of error.

Issued By:

Research Wing CyberPeace Foundation
Research Wing Autobot Infosec Private Ltd.