RESEARCH REPORT ON
FREE 50GB INTERNET DATA
LOCKDOWN OFFER SCAM

CyberPeace Foundation
DISCLAIMER

This report is purely based on technical findings made by the research team during an investigation. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the investigation, information might be changed after generating the reports.
The Research Wing of CyberPeace Foundation has received a message on WhatsApp containing a link which claims that free 50GB internet data is being given to all users as the lockdown offer.

Case Study:

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited have looked into this matter to reach a conclusion that the campaign is either legitimate or an online fraud.

Link:

When the user clicks on the above links they are redirected to https://www.get-free-data[.]xyz/#XX and the following page appears as seen in the screenshot below.

** Where XX represents a unique 13 digits number, for example 1614920821200 and 1614933135000 etc.

![Image of the landing page](image)

The site claims to give free 50 GB data to all the networks mentioned above. On clicking the button shown on the site it asks the respective users to enter their mobile number and to select the network operator.

Also at the bottom of this page a section comes up which seems to be a facebook comment section where many users have commented about how the offer is beneficial.
When the users enter the phone number (here a random number is being given only for the sake of testing) it displays the progress bar and after a while a congratulatory message is displayed and asks users to share the campaign over WhatsApp in order to get benefit.

![FREE 50GB DATA REWARD PORTAL]

Enter your number to check if your Sim Card is Eligible to Receive and Activate free 50GB data plan valid for 2 Months on your mobile phone now.

```
SELECT YOUR NETWORK PROVIDER

ARTEL

1234567890
Send
```

Congratulations! Your Number is Eligible to Receive and Activate free 50GB Data Bundle plan, Valid for 2 Months on your Android Phone or Apple iPhone!

How to activate your free 50GB data plan?
1. To activate your free 50GB data bundle, First click the green button "WHATSAPP" and send this information to 12 groups on WhatsApp!
2. After sending the message, you will now go to the next step where you will be able to complete your free 50GB data activation and receive it on your Mobile within 5 minutes.

Share with your groups

![WhatsApp]

Where the user clicks on the button as seen in the above screenshot, it moves the progress bar and then an error message is displayed as seen in the screenshot below.

![FREE 50GB DATA REWARD PORTAL]

Data Activation Processing...

Processing...

Activating 50GB Data...

100%

100%

Congratulations! Your Number is Eligible to Receive and Activate free 50GB Data Bundle plan, Valid for 2 Months on your Android Phone or Apple iPhone!

How to activate your free 50GB data plan?
1. To activate your free 50GB data bundle, First click the green button "WHATSAPP" and send this information to 12 groups on WhatsApp!
2. After sending the message, you will now go to the next step where you will be able to complete your free 50GB data activation and receive it on your Mobile within 5 minutes.

Sharing failed! The same group or the same friend is invited. Please check and share again.

OK

Once the user clicks OK, one more congratulatory message appears and it asks the user to select the type of device that the user wants to recharge.
Congratulations, you received free 50GB Data bundle plan for your mobile number. To facilitate the activation of your free 50GB data bundle you must complete this final step of Human Verification!

1. You need to be careful to carry out tasks that you will be told according to your mobile system. (Note that this step is important for the option of free 50GB data to work.)

Now Select your Mobile Device.

[Buttons: IPHONE, ANDROID, SMART PHONE]

After clicking any of these buttons it redirects users to Google Playstore url to download an application.

In Depth Analysis:

Some key findings can be mentioned as:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>get-free-data[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>142.250.217.147</td>
</tr>
<tr>
<td>ISP</td>
<td>Google</td>
</tr>
<tr>
<td>ASN</td>
<td>15169</td>
</tr>
<tr>
<td>Country</td>
<td>United States 🇺🇸</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>
Domain Name: GET-FREE-DATA.XYZ
Registry Domain ID: D234292314-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://namecheap.com
Registrar: Namecheap
Registrar IANA ID: 1068

Updated Date: 2021-05-19T14:32:10.0Z
Creation Date: 2021-05-04T11:00:43.0Z
Registry Expiry Date: 2022-05-04T23:59:59.0Z

Registrant State/Province: Capital Region
Registrant Country: IS

Name Server: DNS1.REGRISTRAR-SERVERS.COM
            DNS2.REGRISTRAR-SERVERS.COM

HTTP Response Header:

https://www.get-free-data.xyz

<table>
<thead>
<tr>
<th>HTTP/1.1 200 OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type:</td>
</tr>
<tr>
<td>Expires:</td>
</tr>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>Cache-Control:</td>
</tr>
<tr>
<td>Last-Modified:</td>
</tr>
<tr>
<td>X-Content-Type-Options:</td>
</tr>
<tr>
<td>X-XSS-Protection:</td>
</tr>
<tr>
<td>Server:</td>
</tr>
<tr>
<td>Accept-Ranges:</td>
</tr>
<tr>
<td>Vary:</td>
</tr>
<tr>
<td>Connection:</td>
</tr>
<tr>
<td>Transfer-Encoding:</td>
</tr>
</tbody>
</table>
Source Code Analysis

- Title of the site “FREE 50GB DATA REWARD PORTAL”

- When the user visits the link as seen in the screenshot, a random number is generated.

- A piece of code found that sends an HTTP request to an base64 encoded URL i.e “aHR0cHM6Ly9hcHM6UcmVvcm9zdWlcj5jb20vbG9naW4ucGhhP3drcj16eGNtbmJ2MTI=”. After decoding the URL we found:

  https://aps.reprovides[.]com/login[.]php?wkr=zxcmbv12

- Users are insisted on sharing the campaign with WhatsApp friends and groups.
- The like and comment buttons which are speculated to be of Facebook are static and not dynamic.

```html
 чаt_conversation-box-right {
  margin-left: 20%;
  margin-bottom: 1rem
}

чаt_conversation-box-img {
  width: 3.5rem;
  border-radius: 50%;
  margin-right: 1rem;
  align-self: baseline
}

чаt_conversation-box-active {
  width: 1rem;
  height: 1rem;
  background-color: var(--color-secondary);
  border-radius: 50%;
  position: absolute;
  top: 2.5rem;
  left: 2.7rem
}

чаt_conversation-box-content-comment {
  padding: 1rem;
  background-color: #222;
  border-top-left-radius: 14px;
  border-top-right-radius: 14px;
  border-bottom-left-radius: 14px;
  border-bottom-right-radius: 14px
}

чаt_conversation-box-content-comment-name {
  color: #726695;
  font-weight: 500;
  margin-right: .4rem
}
```

**Piece of HTML code for fake Facebook comment section**
On further investigation, we found a few links related to blogger

```html
<link rel="me" href="https://www.blogger.com/profile/09413084019385763375"/>
<link rel="me" href="https://www.blogger.com/profile/00796980456348365928"/>
<link rel="me" href="https://www.blogger.com/profile/03366061779890292833"/>

-- On visiting the links we are taken to several other blogs
```
- Google Tag Manager config ID found for the site is "G-SVL8VM9819".

```html
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=G-SVL8VM9819"></script>
<script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());

    gtag('config', 'G-SVL8VM9819');
</script>
</script>
```

During the analysis we noticed a domain name https://tuisongxx[.]xyz was mentioned in the source code as a comment on the webpage. Though we found the domain was not reachable at that time.

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>tuisongxx[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status</td>
<td>Not Active</td>
</tr>
</tbody>
</table>

Domain Name: TUISONGXX.XYZ  
Registry Domain ID: D198871398-CNIC  
Registrar WHOIS Server: grs-whois.hichina.com  
Registrar: Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)  
Registrar IANA ID: 1599
App analysis:

Free Internet Data All Network Packages 2021

Case Study:

Upon installing the application it takes the user to the subsequent sections as seen below.
On selecting the ‘ALL NETWORK PACKAGES’ option it displays a List of Network Operators like Jazz, Zong, Telenor etc.

Choosing any of the network operators various options for activating the services are displayed with offers details.
All the offers contain some dialing code for activation of service, so when the user clicks on “ACTIVATE” it redirects the user to the dialer with some predefined dial code.

On selecting the “FREE INTERNET OFFERS” from the first section of the application some questions like Mobile company name, Phone number, whether the number is prepaid or postpaid, Network name are asked to the user.
Finally it displays a Thank You message and asks users to share the app with their friends.

Application Details:

<table>
<thead>
<tr>
<th>App name</th>
<th>SIM Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package name</td>
<td>com.alwahidstudio.paksimpackages.allsimpackages</td>
</tr>
<tr>
<td>Average CVSS Score</td>
<td>7.1</td>
</tr>
<tr>
<td>App Security Score</td>
<td>40/100</td>
</tr>
<tr>
<td>Main Activity</td>
<td>com.alwahidstudio.paksimpackages.allsimpackages.activitySplashActivity</td>
</tr>
<tr>
<td>Target SDK</td>
<td>29</td>
</tr>
</tbody>
</table>
### Play Store Information:

<table>
<thead>
<tr>
<th>Title</th>
<th>Free Internet Data All Network Packages 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Version Support</td>
<td>4.3 and up</td>
</tr>
<tr>
<td>Developer</td>
<td>adventure gang games</td>
</tr>
<tr>
<td>Developer address</td>
<td>633 e 162 street south Holland il - 60473</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:qasimsawna2533@gmail.com">qasimsawna2533@gmail.com</a></td>
</tr>
<tr>
<td>Blog Link</td>
<td><a href="https://dailyallnewspk.blogspot.com">https://dailyallnewspk.blogspot.com</a></td>
</tr>
</tbody>
</table>

### Application Certificate Details:

<table>
<thead>
<tr>
<th>Country</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid from</td>
<td>2021-02-18 10:25:23</td>
</tr>
<tr>
<td>Valid to</td>
<td>2051-02-18 10:25:23</td>
</tr>
<tr>
<td>State</td>
<td>California</td>
</tr>
<tr>
<td>Locality</td>
<td>Mountain View</td>
</tr>
</tbody>
</table>

### Application Permission Details:

```xml
<uses-sdk android:minSdkVersion="18" android:targetSdkVersion="29"/>
<uses-permission android:name="android.permission.CALL_PHONE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<queries>
  <intent>
    <action android:name="android.intent.action.VIEW"/>
    <data android:scheme="https"/>
  </intent>
</queries>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
<queries>
  <intent>
    <action android:name="android.intent.action.VIEW"/>
    <category android:name="android.intent.category.BROWSABLE"/>
    <data android:scheme="https"/>
  </intent>
  <intent>
    <action android:name="android.support.customtabs.action.CustomTabsService"/>
  </intent>
  <intent>
    <action android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
  </intent>
</queries>
```
<table>
<thead>
<tr>
<th>Permission</th>
<th>Status</th>
<th>INFO</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.permissionINTERNET</td>
<td>Dangerous</td>
<td>Full internet access</td>
<td>Allows an application to create network sockets.</td>
</tr>
<tr>
<td>android.permission.CALL_PHONE</td>
<td>Dangerous</td>
<td>Full calling access</td>
<td>Allow an application to initiate a phone call without going through the dialer user interface for the user.</td>
</tr>
<tr>
<td>android.permission.RECEIVE_BOOT_COMPLETED</td>
<td>Normal</td>
<td>Automatically start on boot</td>
<td>Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.</td>
</tr>
<tr>
<td>android.permission.WAKE_LOCK</td>
<td>Normal</td>
<td>Prevent phone from sleep</td>
<td>Allow applications to prevent the phone from sleeping.</td>
</tr>
</tbody>
</table>

The aforementioned permissions are used by the app to perform required operations like View network status, Full internet access, Full calling access etc.
### Basic Properties:

<table>
<thead>
<tr>
<th>File Type</th>
<th>MD5</th>
<th>SHA-1</th>
<th>SHA-256</th>
<th>File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>d8093fc529e15b4f7f656fbe0f69491a</td>
<td>e292188bb77d661f3180e54a8fcedaa17e</td>
<td>38bfa9917bcd11c46990cb2d2ffc7c6c967</td>
<td>10.59 MB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a8efe5</td>
<td>24e5c6635ce78da99ee6f5d79de38</td>
<td>(11104525 bytes)</td>
</tr>
</tbody>
</table>

### IP Lookup:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>dailyallnewspk.blogspot.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>featvpn.com</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Conclusive Summary:

- The campaign is pretended to be an offer from reputed network providers like Airtel, Jio, BSNL or Vodafone but hosted on the third party domain instead of the official website which makes it more suspicious.
- The domain name associated with the campaign has been registered in very recent times.
- The prizes are kept really attractive to lure the laymen.
- The website insist users to share the campaign over WhatsApp however no reputed site would ask its users to share the campaign on WhatsApp.
- The application requires some permission from the users to perform its operations which could be dangerous.

CyberPeace Advisory:

- CyberPeace Foundation recommends that people avoid opening such messages sent via social platforms. One must always think before clicking on such links, or downloading any attachments from unauthorized sources.
- Falling for this trap could lead to whole system compromisation (Access to microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications etc.) as well as financial loss for the users. One must always think before clicking on such links, or downloading any attachments from unauthorized sources.
- Do not share confidential details like login credentials, banking information with such a type of scam.
- Never share or forward fake messages containing links with any social platform without proper verification.

Issued by:

Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Ltd.