Research Report on

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A FREE MOBILE RECHARGE SCAM

WITH THE NAME OF TATA
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 and information might be changed after generating the reports.
RESEARCH REPORT ON

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A FREE MOBILE RECHARGE SCAM WITH THE NAME OF TATA

The Research Wing of CyberPeace Foundation received a message containing a link over WhatsApp which lures users with a free recharge offer of INR 239, pretending to be an offer from TATA on the occasion of Independence Day.

🔗 Link

https://tataoffer[.]site/

🗂️ Summary

⚠️ WARNING SIGNS ⚠️

- The campaign is pretended to be an offer from TATA but is hosted on the third-party domain instead of the official TATA website which makes it more suspicious.
- The domain names associated with the campaign have been registered in very recent times.
- Multiple redirections have been noticed between the links.
- No reputed site would ask its users to share the campaign on WhatsApp.
- The prize is kept really attractive to lure the laymen.
- Grammatical mistakes have been noticed.
- Campaign asks users to install an application from any third party source.

⛅️ CYBERPEACE ADVISORY ⛅️

- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms.
- Falling into this trap could lead to whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as the financial loss for the users.
- Do not share confidential details like login credentials, and banking information with such a type of scam.
- Never share or forward fake messages containing links to any social platform without proper verification.
- There is a need for International Cyber Cooperation between countries to bust the criminal gangs running fraud campaigns affecting individuals and organisations to make Cyberspace resilient and peaceful.
The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited has looked into this matter to reach a conclusion that the website is either legitimate or online fraud.

On Visiting the link users were redirected to

https://tataoffer.site/#XX

**Where XX represents a unique 13 digits number, for example 1660580329852.

On the landing page, there is a tricoloured image wishing users “Happy Independence Day”.

At the bottom of this page, there is a section that seems like a social-media comment section.
The user has to enter the phone number and internet service provider company name.

After selecting and providing any random information one congratulation message gets displayed and asks users to share the campaign over WhatsApp.

“Congratulations, you have got free recharge for 1 month.!

How to activate free recharge.?

1. To activate the free recharge, click on the green "Whatsapp" button below and share this offer with 5 groups or 10 friends in WhatsApp so that they can also take advantage of this offer.!

2. Only after sharing you will be able to go to the next step, which will activate your free recharge for 28 days.!”
After Clicking the WhatsApp button users are given to download apk from a third party.

http://share.royalgame.in/?invite_code=7193492
IN DEPTH INVESTIGATION:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th><a href="https://tataoffer%5B.%5Dsite/">https://tataoffer[.]site/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [OK]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.30.94</td>
</tr>
<tr>
<td>IANA ID</td>
<td>1636</td>
</tr>
<tr>
<td>ASN</td>
<td>13335</td>
</tr>
<tr>
<td>Country</td>
<td>India (IN)</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Domain Name: tataoffer.site

Registrant State/Province: Maharashtra
Registrant Country: India (in)
Registrant Org:

Updated Date: 16/8/2022
Creation Date: 13/8/2022
Registry Expiry Date: 13/8/2023

Name Server: RUDY.NS.CLOUDFLARE.COM
Name Server: ZITA.NS.CLOUDFLARE.COM
In source code analysis we found some information like –

- The title of the page is “TATA OFFER: Free Recharge Offer”

- We found three Google tag manager IDs (G-UA-173027329-1) in the source code.

- The section which seems to be a social media comment area is static and not a dynamic one. The section has been created with some HTML and CSS.
Users are insisted on sharing the campaign with WhatsApp friends and groups.

We got some Chinese language also at the backend of the website as

```javascript
window.open('https://api.whatsapp.com/send?text=15 August 嘿，朋友，不要忘记分享这个活动！
//window.location.href = 'https://api.whatsapp.com/send?text='+ text
}
```

We found a get request is going to this domain(pro.ip-api.com/), this api is used to get the data about users with the city, region, zip, country, continent, timezone, latitude and longitude fields and if users are using anonymous proxies or VPN services.

```javascript
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
  if (xhr.readyState == 4 && xhr.status == 200) {
    var response = JSON.parse(xhr.responseText);
    if (response.status == 'success') {
      console.log('query failed: ' + response.message);
      return;
    }
```
CONCLUSIVE SUMMARY:

The campaign is pretended to be an offer from TATA but is hosted on the third-party domain instead of the official TATA website which makes it more suspicious.

During the investigation we noticed multiple redirections between the links.

We have investigated the URLs in a secured sandbox environment where the WhatsApp application was not installed. If any user opens the link from a device like a smartphone where the WhatsApp application is installed, the sharing features on the site will open the Whatsapp application on the device to share the link.

The prizes are kept really attractive to lure the laymen.

The domain names associated with the campaign have been registered in very recent times.

Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front-end domain names used in this campaign.
CyberPeace Advisory:

CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.

If at all, the user gets into this trap, it could lead to a whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as financial losses.

Do not share confidential details like login credentials, or banking information with such a type of scam.

Do not share or forward fake messages containing links without proper Verification.

Never install an application from a third party source instead of the official app store.

There is a need for International Cyber Cooperation between countries to bust the cybercriminal gangs running the fraud campaigns affecting individuals and organizations, to make Cyberspace resilient and peaceful.

Issued By:

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