RESEARCH REPORT ON

“TATA GROUPS 150TH ANNIVERSARY CELEBRATION”

GIFT SCAM

CyberPeace Foundation
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
“TATA GROUPS. 150TH ANNIVERSARY CELEBRATION” GIFT SCAM.

The Research Wing of CyberPeace Foundation received a link via Whatsapp related to a free gift campaign pretending to be an offer from Tata Groups which asks users to participate in a survey in order to get a chance to win a Tata NEXON EV.

Link:
https://51l[.]org/?1633067710853

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 website is either legitimate or an online fraud.

On Visiting the link users were redirected to the link
https://51l[.]org/?1633067710853#XX

**Where XX represents a unique 13 digits number, for example 1633075913900

On the landing page a Congratulations message appears with an attractive photo of a Tata car and asks users to participate in a quick survey in order to get a “Tata Nexon EV”.

---

CyberPeace Research
Also at the bottom of this page a section comes up which seems to be a comment section where many users have commented about how the offer is beneficial.

The survey starts with some basic questions like **Do you know Tata Groups?** How old are you? What do you think of Tata groups? Are you male or female? etc

Once the user answers the questions a “congratulatory message” is displayed.
“Congratulations!
Your answer has been saved successfully!

You have a chance to win gifts.
You must select the correct box with your prize inside.
You have 3 attempts. Good luck!”

After Clicking the OK button users are given three attempts to win the prize.

After completing all the attempts it says that the user has won “TATA Nexon EV”.

“Congratulations! You did it! You won TATA Nexon EV”
Clicking on the ‘OK’ button, it instructs users to share the campaign on WhatsApp.

Strangely enough the user has to keep clicking the WhatsApp button until the progress bar completes.

After clicking on the green ‘WhatsApp’ button multiple times it shows a section where again a congratulations appears.
In Depth Investigation:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>51L.ORG</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.26.13.128</td>
</tr>
<tr>
<td>ISP</td>
<td>Cloudflare</td>
</tr>
<tr>
<td>ASN</td>
<td>13335</td>
</tr>
<tr>
<td>Country</td>
<td>United States 🇺🇸</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>

Domain Name: 51L.ORG
Registry Domain ID: D402200000017696775-LROR
Registrar WHOIS Server: whois.godaddy
Registrar URL: http://www.whois.godaddy.com
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146

Updated Date: 2021-10-04T18:09:51Z
Creation Date: 2021-08-30T04:59:23Z
Registry Expiry Date: 2022-08-30T04:59:23Z

Registrant Organization: Repossessed by Go Daddy
Registrant State/Province: AZ
Registrant Country: US

Name Server: NS15.DOMAINCONTROL.COM
Name Server: NS16.DOMAINCONTROL.COM
In source code analysis we found some information like --

- The title of the site is “...”

```html
<title>...</title>
<link rel="icon" href="data:image/ico;...">
<meta name="viewport"
    content="width=device-width, initial-scale=1">
```

- 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.

```html
...<div class="comm_name" style="background-color: #f0f0f0;">Debasmita Barik</div>
</h3>
<p>Can I receive today? Thank you</p>

<svg class="likebar" style="flex:
    <div class="fbblue smaller" style="javascript:void(0);">...</div>
    <span style="background-color: #f0f0f0;">2 minutes ago</span>

...<div class="comm_name" style="background-color: #f0f0f0;">Rajnish Verma</div>
</h3>
<p>Fantastic! I have never won anything before!</p>

<svg class="likebar" style="flex:
    <div class="fbblue smaller" style="javascript:void(0);">...</div>
    <span style="background-color: #f0f0f0;">8 minutes ago</span>
```
In source code analysis we found some information like --

- Users are insisted on sharing the campaign with WhatsApp friends and groups.

```javascript
function shareBtn() {
  var share_num = get_Cookie('prog') == ' 
  share_num++
  if (share_num > g_share_step) {
    share_num = g_share_step;
  }
  lk = 'https://511.org/';
  location.href = 'whatsapp://send?text='
}
```

- Google tag manager ID found “G-Q21V794VMY”.

```html
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());
  gtag('config', 'G-Q21V794VMY');
</script>
```

- We found some Chinese language written in the source code

```javascript
function frame() {
  if (p_s >= p_e) {
    clearInterval(id)
  } else {
    var check = String(p_e).indexOf(".") + 1;//获取小数点的位置
    var count = String(p_e).length - check;//获取小数点后的个数
    if (check > 0) {
      if (1 == count) {
        p_s = accAdd(p_s, 0.1);
      } else {
        p_s = accAdd(p_s, 0.01);
      }
  }

Translation for the word is  “Get the position of the decimal point”
**Important**

During the analysis we found, in the background a javascript code called `hm.js` was being executed from the host `hm.[]baidu[].com` which is a subdomain of Baidu and is used for Baidu Analytics, also known as Baidu Tongji.

*Note:* "Baidu is a Chinese multinational technology company specialising in Internet-related services, products and artificial intelligence, headquartered in Beijing's Haidian district, China."
https://en.wikipedia.org/wiki/Baidu

Query URL: `https://hm.baidu[].com/hm.js?80aed573fcb997b68991fe4b20e7d40a`

```javascript
var _hmt = _hmt || [];
(function() {
    var hm = document.createElement("script");
    hm.src = "https://hm.baidu.com/hm.js?80aed573fcb997b68991fe4b20e7d40a";
    var s = document.getElementsByTagName("script")[0];
    s.parentNode.insertBefore(hm, s);
})();
```
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>hm.baidu.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>103.235.46.191</td>
</tr>
<tr>
<td>ISP</td>
<td>Beijing Baidu Netcom Science and Technology Co.</td>
</tr>
<tr>
<td>ASN</td>
<td>55967</td>
</tr>
<tr>
<td>Location</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

**Domain Name:** baidu.com  
**Registry Domain ID:** 11181110_DOMAIN_COM-VRSN  
**Registrar WHOIS Server:** whois.markmonitor.com  
**Registrar URL:** http://www.markmonitor.com  
**Registrar:** MarkMonitor Inc.  
**Registrar IANA ID:** 292

**Updated Date:** 2021-04-07T12:52:21-0700  
**Creation Date:** 1999-10-11T04:05:17-0700  
**Registrar Registration Expiration Date:** 2026-10-11T00:00:00-0700

**Registrant Organization:** Beijing Baidu Netcom Science Technology Co., Ltd.  
**Registrant State/Province:** Beijing  
**Registrant Country:** CN (China)
Conclusive Summary:

- The campaign is pretended to be an offer from Tata Groups but hosted on the third party domain instead of the official website of Tata Groups which makes it more suspicious.
- During the investigation we have 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 smartphones where 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.
- Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front end domain names used in the Tata Groups. 150th Anniversary Celebration gift scam campaign. But during the phases of investigation, we have identified a domain name that was requested in the background and has been traced as belonging to China.

CyberPeace Advisory:

- CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.
- If at all, user gets into this trap, it could lead to whole system compromise such as access to microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications etc as well as financial losses.
- Do not share confidential details like login credentials, banking information with such a type of scam.
- Do not share or forward fake messages containing links without proper verification.
- 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 the Cyberspace resilient and peaceful.

Issued by:

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