Research Report on

CYBER CRIMINALS LURE INTERNET USERS TO GET INTO A FREE SUBSIDY SCAM WITH THE NAME OF INDIAN RAILWAY, GOVT. OF INDIA.
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 and information might be changed after generating the reports.
RESEARCH REPORT ON

CYBER CRIMINALS LURE INTERNET USERS TO GET INTO A FREE SUBSIDY SCAM WITH THE NAME OF INDIAN RAILWAY, GOVT. OF INDIA.

The Research Wing of CyberPeace Foundation received a link via WhatsApp related to a free scheme pretending to be an offer from the Indian Railways, Government of India.

Link


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 offer is either legitimate or an online fraud.

On visiting the link users were redirected to this link

https://ddhkme.top/ZcEeaYDk/IndianRailways/?_t=1654255547012#XX

**Where XX represents a unique 13 digits number, for example 1654255548069.

On the landing page, at the top there is a logo of the Indian Railway, and a photo of PM Narendra Modi standing beside the Vande Bharat train. Users have to participate in a short quiz to win 6000 rupees.
At the bottom of this page, there is a comment section, where many users have commented about how the offer is beneficial.

The quiz starts with some basic questions like:

Do you know Indian Railways?

How old are you?

What do you think about Indian Railway?

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.
After Clicking the OK button users are given three attempts to win the prizes with multiple gift boxes.

After completing the second attempt it says that the user has won 6000 rupees.

“Congratulations!
You did it! You won 6000 rupee”

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 an instruction has been given in order to get the prize.
Congratulations! The last step:

You must complete this final step!

1. You must register the application below, and it must be opened for 30 seconds after registration.
(Remember, this step is very important)
2. After completing the above actions, please wait for admin to check it, the review will be completed within 24 hours.

Complete registration

At the final step it takes the user through multiple advertisement pages.

IN DEPTH INVESTIGATION:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>transportpreside[.]top</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.73.119</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: transportpreside.top
Registry Domain ID: D20220519G10001G_81533842-top
Registrar WHOIS Server: whois.eranet.com
Registrar URL: http://www.eranet.com
Registrar: Eranet International Limited Registrar
IANA ID: 1868
Updated Date: 2022-05-19T08:12:58Z
Creation Date: 2022-05-19T01:45:46Z
Registry Expiry Date: 2023-05-19T01:45:46Z

Registrant Organization: weiyunlang
Registrant State/Province: GX (Guangxi Zhuang Autonomous Region)
Registrant Country: CN (China)

Name Server: isabel.ns.cloudflare.com
plato.ns.cloudflare.com

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>ddhkmw.[.]top</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.22.245</td>
</tr>
<tr>
<td>ISP</td>
<td>Google-Private-Cloud</td>
</tr>
<tr>
<td>ASN</td>
<td>396982</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>

Domain Name: ddhkmw.top
Registry Domain ID: D20210917G10001G_68994424-top
Registrar WHOIS Server: whois.aliyun.com
Registrar: Alibaba.com Singapore E-Commerce Private
Limited Registrar IANA ID: 3775
Registrar URL: http://www.ali babacom.cloud.com

Updated Date: 2021-09-18T03:56:41Z
Creation Date: 2021-09-17T12:57:17Z
Registry Expiry Date: 2022-09-17T12:57:17Z

Registrant State/Province: jiangsu
Registrant Country: CN (China)

Name Server: camilo.ns.cloudflare.com
irma.ns.cloudflare.com
In source code analysis we found some information like –

- The title of the page is "Indian Railways Government Transport Subsidy!"

- 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.

```javascript
function shareBtn() {
    var share_num = getCookie('prog') == '' ? 0 : parseInt(getCookie('prog'))
    share_num++
    if (share_num > g_share_step) {
        share_num = g_share_step;
    }

    let jurl = j;
    if(nptimes.length > 0){
        if(nptimes.includes(share_num)){
            jurl = j2;
        }
    }

    location.href = 'whatsapp://send?text=' + jurl + new Date().getTime();
    setTimeout(function () {
        getCookie('prog') == '' ? value = 1 : value = parseInt(getCookie('prog'));
        if (value >= g_share_step) {
            continueBtn();
        }
    }, 2000);
}
```

We found three Google tag manager ids:
(G-LW7434MYMN, G-0C230YDF7G, G-RY785CXC08)

```html
<script async src="https://www.googletagmanager.com/gtag/js?id=G-LW7434MYMN"></script>
<script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());
    gtag('config', 'G-LW7434MYMN');
</script>

<script async src="https://www.googletagmanager.com/gtag/js?id=G-0C230YDF7G"></script>
<script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());
    gtag('config', 'G-0C230YDF7G');
</script>

```html
<script data-cfasync="false" src="https://cnd-cgi/scripts/5c5dd728/cloudflare-static/email-decode.min.js"></script>
<script>
    window.dataLayer = window.dataLayer || [];
    function gtag(){dataLayer.push(arguments);}
    gtag('js', new Date());
    gtag('config', 'G-RY785CXC08');
</script>
```

In source code analysis we found some javascript functions that collect the browser and system information from the user's device.
In background this site is sending GET requests to many domains like:

**uprimp.com**

```
GET /br.php?section=general&pub=593174&format=388x58&g=1 HTTP/1.1
Host: uprimp.com
Cookie: used_od2833388e=3; total_impressions=3; cpa.663459=388x58.671757614.0
User-Agent: Mozilla/5.0 (Linux; Android 12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.4864.127 Mobile Safari/537.36
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dnkmw.top/
Sec-Fetch-Mode: script
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```

**qoaaa.com**

```
GET //f4ed86e6be6c/1f5f9451684/?placementName=Adver&randomAd_72122&maxwell=0 HTTP/2
Host: qoaaa.com
User-Agent: Mozilla/5.0 (Linux; Android 12) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.4864.127 Mobile Safari/537.36
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://dnkmw.top/RtEq7aW/IndianRailways/?_t=1654266346064
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Te: trailers
```
**Important**

During the analysis, we found some javascript code in the background 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 specializing in Internet Related services, products, and artificial intelligence, headquartered in Beijing's Haidan district, China."

https://en.wikipedia.org/wiki/Baidu
Domain Name: baidu.com
Registry Domain ID: 111811110_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292

Updated Date: 2022-01-25T09:23:56+0000
Creation Date: 1999-10-11T11:05:17+0000
Registrar Registration Expiration Date: 2026-10-11T07:00:00+0000

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 Indian Railways but hosted on the third party domain instead of the official website of Indian Railways 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.

The domain names used in the campaign have been registered recently.

Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front end domain name used in the 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 cyber-criminal gangs running the fraud campaigns affecting individuals and organisations, to make the Cyberspace resilient and peaceful.

Issued by:

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