RESEARCH REPORT ON THE FRAUD HAPPENING WITH THE NAME OF UOB INVESTMENT IN 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, information might be changed after generating the reports.
RESEARCH REPORT ON THE FRAUD HAPPENING WITH THE NAME OF UOB INVESTMENT IN INDIA

One of the CyberPeace Corps Volunteers has asked the Research Wing of CyberPeace Foundation to initiate an investigation on a link which asks users which claims users can earn more than INR 100000 by UOB investment in India.

![Image of the link]

Any one kindly decode this link. It's looks like suspicious. From different numbers this kind of links send to the users.

![Image of confirming collecting money]

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:

http://vip.]71lou[.]com/

On the landing page it describes users about the scheme. Also there was a Contact Us button at the bottom of the page.
On clicking the Contact Us button it redirected us to api.whatsapp.com.

In Depth Analysis

Below are some of the key findings --

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>vip.71lou.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>47.241.9.153</td>
</tr>
<tr>
<td>ISP</td>
<td>Alibaba</td>
</tr>
<tr>
<td>ASN</td>
<td>45102</td>
</tr>
<tr>
<td>Country</td>
<td>Singapore</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Domain name: 71lou.com
Registry Domain ID: 2532170345.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.bizcn.com
Registrar URL: http://www.bizcn.com
Registrar: Bizcn.com, Inc.
Registrar IANA ID: 471

Updated Date: 2021-05-07T17:17Z
Creation Date: 2020-05-31T02:13:26Z
Registrar Registration Expiration Date: 2021-05-31T02:13:26Z
Registrant State/Province: Zhe Jiang
Registrant Country: CN (China)

Name Server: jm1.dns.com
jm2.dns.com

Phone number: +447459945336

<table>
<thead>
<tr>
<th>Points</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number</td>
<td>+447459945336</td>
</tr>
<tr>
<td>Country</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Country code</td>
<td>44</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Eastern European Time (EET)</td>
</tr>
</tbody>
</table>

Further we have verified the number to check whether it is linked with any social media account on reputed platforms like Google, Facebook, Whatsapp, Twitter, Instagram and Linkedin.

As of now the time of the report is being written we found the number is linked with Google, Facebook, WhatsApp and Twitter.

<table>
<thead>
<tr>
<th>Social Platform</th>
<th>Account Existence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Yes</td>
</tr>
<tr>
<td>Whatsapp</td>
<td>Yes</td>
</tr>
<tr>
<td>Facebook</td>
<td>Yes</td>
</tr>
<tr>
<td>Twitter</td>
<td>Yes</td>
</tr>
<tr>
<td>Instagram</td>
<td>No</td>
</tr>
<tr>
<td>Linkedin</td>
<td>No</td>
</tr>
</tbody>
</table>
We found the profile picture of the WhatsApp account.

![Profile Picture](image_url)

Mute notifications
Custom notifications
Media visibility
Disappearing messages
Encryption
Messages and calls are end-to-end encrypted. Tap to verify.
About and phone number
Take every day seriously
6 May

After doing the reverse image search of the image we found that the image is taken from the internet.

![Sites with information about the image](image_url)

Note: We also have noticed that the number varies on the basis of the Location of the User.

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.”

<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 Domain name used in the campaign has the registrant's country as China.
- It has been noticed that the number varies on the basis of the Location of the User.
- We have investigated the url in a secured sandbox environment where WhatsApp application was not installed. If any user opens the link from a device like smartphones where WhatsApp application is installed the link will open the chat window of the respective number on WhatsApp application.
- During the analysis it has been 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.
- The investigation can be further proceeded after getting engaged with the person behind the WhatsApp chat.

CyberPeace Advisory:

- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms. One must always think before clicking on such links or downloading any attachments from unauthorised sources.
- Do not share confidential details like login credentials, banking information with such types of scams.
- 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.