RESEARCH REPORT ON
FREE GIFT OF Rs. 50,00,000
FROM STATE BANK OF INDIA - SCAM
The Research Wing of CyberPeace Foundation received a link via WhatsApp related to a Free gift campaign pretending to be an offer from State Bank of India.

Link:

https://jccyhc[.]bar/tb.php?app=sbi

Case Study:

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

On visiting the link users were redirected to the link https://sxceod[.]shop/?app=sbi#

On the landing page a congratulations message appears with an attractive photo of State Bank of India and asks users to participate in a quick survey to get a free gift of INR 5000000 from the State bank of India.
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.

The survey starts with some basic questions like **Do you want a gift?, How old are you?, How do you rate State Bank of India services?, Are you an adult? etc.**

Once the user answers the questions a “congratulatory message” is displayed

“Congratulations, your answers have been successfully saved!

You have a chance to win rewards.
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 Rs. 5000000.

"Congratulations! You did it! You won the ₹5000000!"

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 to complete registration in order to get the prize.
After clicking on the green ‘Complete registration’ button, it redirects the user to multiple advertisements webpages and it varies each time the user clicks on the button.

**In Depth Investigation:**

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>jccyhc[.]bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.47.23</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:** JCCYHC.BAR  
**Registry Domain ID:** D230638429-CNIC  
**Registrar WHOIS Server:** whois.rrproxy.net  
**Registrar URL:** http://www.key-systems.net

**Registrar:** Key-Systems LLC  
**Registrar IANA ID:** 1345
Updated Date: 2021-06-17T09:35:36.0Z
Creation Date: 2021-03-31T01:53:14.0Z
Registry Expiry Date: 2022-03-31T23:59:59.0Z

Registrant Country: CN (China)
Name Server: NS2.DOMAINS-HOLD.COM
               NS1.DOMAINS-HOLD.COM

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>sxceed[.]shop</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.63.154</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: SXCEED.SHOP
Registry Domain ID: D05671844-GMO

Registrar WHOIS Server: whois.dnspod.cn
Registrar URL: https://www.dnspod.cn
Registrar: DNSPod, Inc.
Registrar IANA ID: 1697
Registrar Abuse Contact Email: abuse@dnspod.com
Registrar Abuse Contact Phone: +86.4009100100

Updated Date: 2021-06-18T02:02:28.0Z
Creation Date: 2021-04-23T06:17:12.0Z
Registry Expiry Date: 2022-04-23T23:59:59.0Z

Registrant State/Province: guang dong
Registrant Country: CN (China)

Name Server: AMIT.NS.CLOUDFLARE.COM
              MALEAH.NS.CLOUDFLARE.COM
In source code analysis we found some information like --

- The title of the site is "State Bank of India gift 🎁".

- 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.
In source code analysis we found some information like –

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

```javascript
var url_share = items[share_num]['share_link']
var share_text = items[share_num]['share_desc']
var randomItem = share_text + " " + url_share

window.open('whatsapp://send?text=' + randomItem)
```

- Several related links were found in code.
  
  
  https://ghtsmlx.vip/tb.php?app=sbi

- Google tag manager ID found “UA-186893005-2”.
  
  ```html
  <script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}  
  gtag('js', new Date());
  
  gtag('config', 'UA-186893005-2');
  </script>
  ```

- In further source code analysis we found that all the gifts choosing, surveys, the prize winning sections, blue progress bar present on site are statically programmed.
Congratulations, your answers have been successfully saved!

You have a chance to win rewards.

You must select the correct box with your prize inside.

You have 3 attempts. Good luck!

---

Congratulations! You did it! You won the ₹5000000!

Congratulations! The last step:

You must complete this final step:

1. You must register the application below, and it must be opened (Remember, this step is very important)

---

**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.”

Query URL: https://hm.baidu.com/hm.js?c253da48e0531fae8c003d0673a0ac3f

```javascript
(function() {
  var hm = document.createElement("script");
  hm.src = "https://hm.baidu.com/hm.js?c253da48e0531fae8c003d0673a0ac3f";
  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 State Bank of India but hosted on the third party domain instead of the official website of State Bank of India 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 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 prize is kept really attractive to lure the laymen.

- All the domain names associated with the campaign have the registrant country as China.

- Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front end domain names used in this Free gifts from SBI 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 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 compromise (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.