Research Report on:
“SBI - Earn Redeem Points” Phishing
DISCLAIMER

This report is based on purely technical findings made by the research team during the investigation. It is not intended to malign or in any way target any country, actor or person through the findings. All the information provided in the report has been extracted during the investigation.
The Research Wing at CyberPeace Foundation has received an sms asking users to redeem SBI credit points worth INR 9870/- by clicking on a suspicious link.

Link:


Case Study:


On the landing page, a "State Bank of India Fill your Details" form appears which asks users to submit their personal information like Name, Registered Mobile No, Email, Email Password, Date of Birth, Card Number, Expiry Date, CVV, Mpin.
After submitting the details it redirects users to the Thank you page.

Thank You

**In Depth Investigation:**

The Research wing at CyberPeace foundation along with the Research wing of Autobot Infosec Private Limited started an in-depth investigation on the link to come to a conclusion that the website is either legitimate or an online fraud.

Some key findings can be mentioned as:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>earncreditreempoint[.]com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>103.86.177.98</td>
</tr>
<tr>
<td>ISP</td>
<td>Web Werks India Pvt.</td>
</tr>
<tr>
<td>ASN</td>
<td>9583</td>
</tr>
<tr>
<td>Country</td>
<td>India</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>
Registry Domain ID: 2588450902_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Updated Date: 2021-02-01T08:22:40Z
Creation Date: 2021-02-01T07:22:38Z
Registry Expiry Date: 2022-02-01T07:22:38Z
Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Registrant Organisation: sanjay bags
Registrant State: Tamil Nadu
Registrant Country: IN (India)
Name Servers: ns115.herosite.pro
ns114.herosite.pro

[**Registrant**: The person or the entity actually registered the domain.]

HTTP Header Response

http://earncreditcredempoint[.]com

<table>
<thead>
<tr>
<th>HTTP/1.1 200 OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection:</td>
</tr>
<tr>
<td>Content-Type:</td>
</tr>
<tr>
<td>X-UA-Compatible</td>
</tr>
<tr>
<td>Link:</td>
</tr>
<tr>
<td>Link:</td>
</tr>
<tr>
<td>Link:</td>
</tr>
<tr>
<td>Transfer-Encoding:</td>
</tr>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>Server:</td>
</tr>
<tr>
<td>Vary:</td>
</tr>
</tbody>
</table>
In source code analysis we found some information like:

- Title name of the site is 'Home - Earn Redeem Points'.

- Image used on the landing page is taken from link http://earncreditreseedpoint[,]com/wp-content/uploads/2021/02/SBI-Profile.png

- Found tag <link rel='dns-prefetch' href='//s.w.org' /> in the source code. The s.w.org redirect users to https://wordpress.org/ which indicates that the website is built with wordpress.
By visiting the [http://earncreditredempoint[].com/feed/](http://earncreditredempoint[].com/feed/) we downloaded a file called wXZUI3aw. Some information has been extracted by reading the file, like site name, lastBuildDate, wordpress version used etc.

We found a link [earncreditredempoint[].com/wp-json/](http://earncreditredempoint[].com/wp-json/) which gives the details about which functionalities are being used by the site.
- During the investigation we noticed, the form takes the user inputs without performing some basic validation of data type.

For example the **Registered Mobile No.** field should take only numerical values but it accepts user input in text also. It can also be confirmed from the source code where the input type of the field is mentioned as 'text' instead of 'number' or 'tel'.

The **Email Password** field shows the entered password in clear text during the form fill up, it should have been hidden. Again in the source code it can be seen the input type of the field is mentioned as 'text' instead of 'password'.
Likewise the **Card Number** field accepts the infinite digits whereas the SBI cards usually have 16 digits card numbers.

All these kinds of negligence clearly indicates the bad practise of coding.

- On clicking the submit button after filling the form, it passes the data through `/wp-json/contact-form-7/v1/contact-forms/24/feedback` using POST method.

```plaintext
POST /wp-json/contact-form-7/v1/contact-forms/24/feedback HTTP/1.1
Host: earncreitreedepoint.com
Content-Length: 1638
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Origin: http://earncreitreedepoint.com
Referer: http://earncreitreedepoint.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US, en;q=0.9
Connection: close
```

As a response it redirects to the [http://earncreitreedepoint.com/thankyou/](http://earncreitreedepoint.com/thankyou/) page following a thank you message as "Thank you for your message. It has been sent."
Technologies used:

Website is developed using **wordpress version 5.6.1**

- WordPress theme in use: **sinatra**

- Latest Version: 1.1.6 (up to date)
- Last Updated: 2021-01-07T00:00:00Z
- Readme: [http://earncreditreedempoint[.]com/wp-content/themes/sinatra/readme.txt](http://earncreditreedempoint[.]com/wp-content/themes/sinatra/readme.txt)

--- Sinatra ---
Contributors: sinatra team

Tags: two-columns, right-sidebar, left-sidebar, footer-widgets, blog, news, custom-background, custom-menu, post-formats, sticky-post, editor-style, threaded-comments, translation-ready, custom-colors, featured-images, full-width-template, microformats, theme-options, e-commerce

Requires at least: 5.8
Tested up to: 5.9
Requires PHP: 5.6
License: GPL2 or later
License URI: [http://www.gnu.org/licenses/gpl-2.0.html](http://www.gnu.org/licenses/gpl-2.0.html)
Stable tag: trunk

A lightweight and highly customizable multi-purpose theme that makes it easy for anyone to create their perfect website.

--- Description ---
Sinatra is a lightweight and highly customizable multi-purpose theme that makes it easy for anyone to create their perfect website. It comes with microdata integration, unlimited colors, multiple layouts, pre-built demo websites and so much more. It is also translatable and built with best SEO practices. It works well with your favorite plugins such as: WooCommerce, JetPack, page builders, SEO plugins and others.

--- Style URL ---
[http://earncreditreedempoint[.]com/wp-content/themes/sinatra/style.css](http://earncreditreedempoint[.]com/wp-content/themes/sinatra/style.css)

- Style Name: Sinatra
- Description: Sinatra is a lightweight and highly customizable multi-purpose theme
- Author: Sinatra Team
## Plugins used by site

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Form 7</td>
<td>5.3.2</td>
<td>This plugin is used for creating the form to take details.</td>
</tr>
<tr>
<td>Elementor</td>
<td>3.1.1</td>
<td>The purpose of the plugin is to implement good design in the UI of a site.</td>
</tr>
<tr>
<td>Material Design for Contact Form 7</td>
<td>2.6.4</td>
<td>It is used to make the contact form more interactive.</td>
</tr>
<tr>
<td>Wordpress-SEO</td>
<td>15.7</td>
<td>To optimize the search results in search engines.</td>
</tr>
<tr>
<td>wpcf7-redirect</td>
<td>2.3.3</td>
<td>Main purpose of the plugin is to redirect the links internally to some other sites like bit.ly to earn redeem.</td>
</tr>
</tbody>
</table>

We found the wordpress administrative login page of the site by visiting the url -
http://earncreditreempoint[.]com/wp-admin
During the investigation on the site we found that it has XML-RPC enabled which might tend the site to be vulnerable with pingback attack and brute force attack via XML-RPC.

XML-RPC on WordPress is actually an API that allows developers who make 3rd party applications and services to have the ability to interact with the WordPress site. The XML-RPC API provides several key functionalities that include Publish a post, Edit a post, Delete a post, Upload a new file (example: an image for a post), Get a list of comments, Edit comments.

Conclusive Summary:

- According to the State bank of India, they never communicate with customers through sms, mail containing links regarding any account related staff.

- The site is collecting the data directly without any verification which makes it a bit suspicious.

- The site is registered by a third party instead of having the registrant organisation name as State bank of India.

- Usually any reputed Banking entity does not use Wordpress like CMS technologies on their official website for security reasons.

Issued By:

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