Research Report on

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A BRANCH PROMOTION BONUS OF INR 6000 SCAM

WITH THE NAME OF HALDIRAM’S
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.
The Research Wing of CyberPeace Foundation received a message over Whatsapp containing a suspicious link that lures users with branch opening promotion pretending to be an offer from Haldiram’s.

[Link]

Summary

[Warning Signs]
- The campaign is pretended to be an offer from Haldiram’s Branch but is hosted on the third-party domain instead of the official website of Haldiram’s which makes it more suspicious.
- The domain names associated with the campaign have been registered in very recent times.
- Multiple redirections have been noticed between the links.
- No reputed site would ask its users to share the campaign on WhatsApp.
- The prize is kept really attractive to lure the laymen.
- Grammatical mistakes have been noticed.

[Cyberpeace Advisory]
- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms.
- Falling into this trap could lead to whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as the financial loss for the users.
- Do not share confidential details like login credentials, and banking information with such a type of scam.
- Never share or forward fake messages containing links to any social platform without proper verification.
- There is a need for International Cyber Cooperation between countries to bust the criminal gangs running fraud campaigns affecting individuals and organisations to make Cyberspace resilient and peaceful.
Case Study

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited has looked into this matter to reach a conclusion that the website is either legitimate or online fraud.

On Visiting the link users were redirected to https://pjc0pq[].cn/ZDKUdtVo/Haldiram-qf/?_t=1661164305207#XX

**Where XX represents a unique 13 digits number, for example 1661165003471.

On the landing page, there is an image of Haldiram’s Branch Outlet with other members and a message that says (Through the questionnaire, you will have a chance to get 6000 rupees.)

At the bottom of this page, there is a section that seems like a social-media comment section where many people have commented on how the offer is beneficial.

- Aparna Sukesh:
  I thought it was a joke, but it was delivered this morning! So surprised! @Apotol is the best company I've ever met!
  ![Thumb up emoji]
  1 minute ago

- Sai Sanjeev Reddy:
  I can't believe it! I won a gift! Thanks @Apotol 😊😊
  ![Thumb up emoji]
  3 minutes ago

- Shivaraj N Pratiksha:
  Great, I never win anything. I'm amazed, thanks Apotol for the anniversary gift! 😊😊
  ![Thumb up emoji]
  7 minutes ago

- Shabbir Ahmed:
  Thanks @Apotol Hospital! Really, I got a gift; I told my friends about it so they can get it too!
  ![Thumb up emoji]
  9 minutes ago
The user has to answer four questions to win the gift. It starts with some basic questions like

“Do you know Haldiram’s?
How old are you?
How do you think of Haldiram’s?
Are you male or female?” etc.

After answering all four questions a congratulatory message appears.

“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 prizes with multiple gift boxes.

On the 2nd attempt, it says that the user has won INR 6000.
**Note:** During our investigation we noticed the currency varies based on the location of the user. For an example if the user visits the url from India, it shows the winning prize in INR but if the url is being visited from a different country say Switzerland, it shows the prize in Franken.

"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 click the WhatsApp button until the blue bar reaches 100%.
After clicking the Continue button, a new box appears, here the user has to complete registration according to the given steps.

Your prize is: 6000 Rupee. Follow the instructions on the next page to claim your 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

When the user clicks on the **Complete registration** button it redirects users to multiple advertisement pages and it varies every time the user visits the URL.
IN DEPTH INVESTIGATION:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th><a href="http://lowpricesclub.com">http://lowpricesclub.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ OK ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.147.144</td>
</tr>
<tr>
<td>ASN</td>
<td>13335</td>
</tr>
<tr>
<td>Country</td>
<td>Michigan - Burt</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Domain Name: lowpricesclub.com
Registrar URL: http://www.ordertld.com
Registrar: CNOBIN INFORMATION TECHNOLOGY LIMITED
Registrar IANA ID: 3254

Updated Date: 2021-12-25T04:23:11Z
Creation Date: 2021-12-25T00:00:00Z
Registry Expiry Date: 2022-12-25T00:00:00Z

Registrant State/Province: shaan xi
Registrant Country: CN (China)

Name Server: GLEN.NS.CLOUDFLARE.COM
Name Server: TINA.NS.CLOUDFLARE.COM
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>pjc0pq.cn/[.]cn/</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ OK ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.49.121</td>
</tr>
<tr>
<td>ISP</td>
<td>Cloud flare</td>
</tr>
<tr>
<td>ASN</td>
<td>13335</td>
</tr>
<tr>
<td>Country</td>
<td>China</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Domain Name: pjc0pq.cn  
ROID: 20220717s10001s48552875-cn  
Domain Status: ok

Registration Time: 2022-07-17 19:11:17  
Expiration Time: 2023-07-17 19:11:17

Registrant: 刘甜甜 (Liu Tiantian)  
Registrant Contact Email: evgeniyapbn5gle@mail.ru  
Sponsoring Registrar: 阿里云·算有限公司（万网） (Alibaba Cloud Computing Co., Ltd. (Wanwang))

Name Server: davina.ns.cloudflare.com  
Name Server: marty.ns.cloudflare.com
In source code analysis we found some information like -

- The title of the page is “Haldiram’s Branch opening promotion!”

- We found three Google tag manager ids (G-SLR621WYP, G-LW7434MYMN and G-0C230YDF7G) in the source code.
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
jurl = j2;

location.href = `whatsapp://send?text= + jurl + new Date().getTime();

setTimeout(function () {
    getCookie('prog') == '' ? value = 1 : value = parseInt(get_Cookie('prog'));
    if (value >= q_share_step) {
        continueBtn();
    } else
        value == 2 || value == 4 ? swal('The same group or the same friend is not
```

In background analysis we found that this website is sending requests to other domains like uprmp.com qoaaa.com

```html
  data domain="/qoaaa.com" data-aquery="/koqaa.png" data-url="/koqaa.png" data-src="/koqaa.png" async
  type="Text/javascript" src="http://uprmp.com/hr-corp/section GENERATOR/3001746/format/3001746/code/scripture/divs/counter.js"
```

We found some Chinese language written in the source code.

```javascript
function getMainHost() {
// 获取主域名
  let key = Math.random();
  let key = RegExp('(');\{s\}(key)+12345\});
  let expiredtime = new Date(0);
  let domain = document.domain;
  let lanlist = domain.split('');
  while (domainlist.length) {
      let domainlist = domainlist.pop();
      while (domainlist.length) {
```
In source code analysis we found some javascript functions that collect the browser and system information from the user's device.

```javascript
function getBrowser() {
    if (navigator.userAgent.indexOf('opera') != -1) {
        return 'Opera';
    } else if (navigator.userAgent.indexOf('chrome') != -1) {
        return 'Google Chrome';
    } else if (navigator.userAgent.indexOf('Safari') != -1) {
        return 'Safari';
    } else if (navigator.userAgent.indexOf('Firefox') != -1) {
        return 'Firefox';
    } else if (navigator.userAgent.indexOf('MSIE') != -1) {
        return 'IE';
    } else {
        return 'Unknown';
    }
}

function getPlatform() {
    if (window.navigator.userAgent.indexOf('Windows NT 10.0') != -1) {
        return 'Windows 10';
    }
    if (window.navigator.userAgent.indexOf('Windows NT 6.2') != -1) {
        return 'Windows 8';
    }
    if (window.navigator.userAgent.indexOf('Windows NT 6.1') != -1) {
        return 'Windows 7';
    }
    if (window.navigator.userAgent.indexOf('Windows NT 6.0') != -1) {
        return 'Windows Vista';
    }
    if (window.navigator.userAgent.indexOf('Windows NT 5.1') != -1) {
        return 'Windows XP';
    }
    if (window.navigator.userAgent.indexOf('Windows NT 5.0') != -1) {
        return 'Windows 2000';
    }
    if (window.navigator.userAgent.indexOf('iPhone') != -1) {
        return 'iPhone';
    }
    if (window.navigator.userAgent.indexOf('iPad') != -1) {
        return 'iPad';
    }
    if (window.navigator.userAgent.indexOf('Android') != -1) {
        return 'Android';
    }
    if (window.navigator.userAgent.indexOf('Mac') != -1) {
        return 'Macintosh';
    }
}
```

**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 specializing in Internet-related services, products, and artificial intelligence, headquartered in Beijing’s Haidian district, China.”
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: 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 Haldiram’s but hosted on the third-party domain instead of the official website of Haldiram’s 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 a smartphone where the 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.

Both the domain names used in this campaign have the registrant country as China.

The domain names associated with the campaign have been registered in very recent times.

Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front-end domain names used in this gift scam campaign. But during the phases of the 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, the user gets into this trap, it could lead to a whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as financial losses.

Do not share confidential details like login credentials, or 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 organizations, to make Cyberspace resilient and peaceful.

Issued By:

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