RESEARCH REPORT ON
“FLIPKART 15TH ANNIVERSARY” FREE GIFTS SCAM
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
“FLIPKART 15TH ANNIVERSARY”
FREE GIFTS SCAM

The Research Wing of CyberPeace Foundation received a link via WhatsApp related to a Free gift campaign pretending to be an offer from Flipkart which asks users to participate in a survey to have a chance to win a Mi 11 Lite mobile phone.

Link:
https://fkryrq[.]work/flipkarttest/tb.php?_t=16252179221625218120742

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 website is either legitimate or an online fraud.

On visiting the link users were redirected to the link
https://fdfer[.]bar/flipkarttest/?_t=1625292236500#XX

** Where XX represents a unique 13 digits number, for example 1614920821200 and 1614933135000 etc.

On the landing page a congratulations message appears with an attractive photo of Mi 11 Lite Mobile phone and asks users to participate in a quick survey to get a Mi 11 Lite phone.
Also at the bottom of this page a section comes up which seems to be a comment section where many users have commented about how the offer is beneficial.

The survey starts with some basic questions like **Do you know Flipkart?, How old are you?, How do you think of Flipkart?, 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.
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 “Mi 11 Lite (Tuscany Coral, 128 GB)”.

“Congratulations! You did it! You won Mi 11 Lite (Tuscany Coral, 128 GB)”
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>fkryrq[.]work</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.86.11, 172.67.213.188</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: FKRYRQ.WORK
Registry Domain ID: D_021F8A58_67888A28CCD34465B99E24ECD79CE5FA_0000017A2DD05041-WORK

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

Updated Date: 2021-07-01T11:29:22Z
Creation Date: 2021-06-21T09:04:24Z
Registry Expiry Date: 2022-06-21T09:04:24Z

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

Name Server: lee.ns.cloudflare.com.
             chin.ns.cloudflare.com.
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>fdfer[.]bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.137.244, 104.21.78.229</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: FDFER.BAR
Registry Domain ID: D218761348-CNIC

Registrar WHOIS Server: whois.rrproxy.net
Registrar URL: http://www.key-systems.net
Registrar: Key-Systems LLC
Registrar IANA ID: 1345

Updated Date: 2021-07-02T12:01:06.0Z
Creation Date: 2021-01-22T15:49:39.0Z
Registry Expiry Date: 2022-01-22T23:59:59.0Z

Registrant Country: CN (China)

Name Server: DYLAN.NS.CLOUDFLARE.COM
             ROSE.NS.CLOUDFLARE.COM
HTTP Response Header:

https://fdfer[.]bar/flipkarttest/?_t=1625292236500#1625292241000

<table>
<thead>
<tr>
<th>HTTP/1.1 200 OK</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>Mon, 05 Jul 2021 10:25:35 GMT</td>
</tr>
<tr>
<td>Content-Type:</td>
<td>text/html; charset=UTF-8</td>
</tr>
<tr>
<td>Transfer-Encoding:</td>
<td>chunked</td>
</tr>
<tr>
<td>Connection:</td>
<td>close</td>
</tr>
<tr>
<td>Vary:</td>
<td>Accept-Encoding</td>
</tr>
<tr>
<td>CF-Cache-Status:</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>Report-To:</td>
<td>{&quot;endpoints&quot;: [{&quot;url&quot;: &quot;<a href="https://Wa.nel.cloudflare.com/report/vv2?v2=s=I79y9wIFYD%2FLKhalvdbFmvAidWW%2FHmc3Ca69UBYNh6rqz01lCX6Dvoa7TnbT%2BEpSUKdrpnADDy97bktifbMUT88qd8H3qaYHAcq02uSLqTEUEYBWu9G%22%7D">https://Wa.nel.cloudflare.com/report/vv2?v2=s=I79y9wIFYD%2FLKhalvdbFmvAidWW%2FHmc3Ca69UBYNh6rqz01lCX6Dvoa7TnbT%2BEpSUKdrpnADDy97bktifbMUT88qd8H3qaYHAcq02uSLqTEUEYBWu9G&quot;}</a>, &quot;group&quot;: &quot;cf-nel&quot;, &quot;max_age&quot;: 604800}</td>
</tr>
<tr>
<td>NEL:</td>
<td>{&quot;report_to&quot;: &quot;cf-nel&quot;, &quot;max_age&quot;: 604800}</td>
</tr>
<tr>
<td>Server:</td>
<td>cloudflare</td>
</tr>
<tr>
<td>CF-RAY:</td>
<td>669fe3e5a85257af-IAD</td>
</tr>
<tr>
<td>alt-svc:</td>
<td>h3-27: &quot;443&quot;, ma=86400, h3-28: &quot;443&quot;, ma=86400, h3-29: &quot;443&quot;, ma=86400, h3: &quot;443&quot;, ma=86400</td>
</tr>
</tbody>
</table>
In source code analysis we found some information like --

- The title of the site is “Flipkart 15th Anniversary! 🎉.”

- 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;
    }
    location.href = 'whatsapp://send?text=' + j + new Date().getTime();
}
```

Google tag manager ID found “G-ZBWD66MKXC”.

```html
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'G-ZBWD66MKXC');
</script>
```

The campaign collects browser data and system data from the 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";
    } else if (window.navigator.userAgent.indexOf("Windows NT 6.2") != -1) {
        return "Windows 8";
    } else if (window.navigator.userAgent.indexOf("Windows NT 6.1") != -1) {
        return "Windows 7";
    } else if (window.navigator.userAgent.indexOf("Windows NT 6.0") != -1) {
        return "Windows Vista";
    } else if (window.navigator.userAgent.indexOf("Windows NT 5.1") != -1) {
        return "Windows XP";
    } else if (window.navigator.userAgent.indexOf("Windows NT 5.0") != -1) {
        return "Windows 2000";
    } else if (window.navigator.userAgent.indexOf("Mac") != -1) {
        return "Macintosh";
    } else if (window.navigator.userAgent.indexOf("iPhone") != -1) {
        return "iPhone";
    } else if (window.navigator.userAgent.indexOf("iPad") != -1) {
        return "iPad";
    } else if (window.navigator.userAgent.indexOf("Android") != -1) {
        return "Android";
    } else {
        return "Others";
    }
}
```
**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.”

https://en.wikipedia.org/wiki/Baidu

Query URL: `https://hm.baidu[.]com/hm.js?e83e4356fef9cf79862cf48ca0ec0237`
`https://hm.baidu.com/hm.js?fe2131a30a7eef80970fad70159cd124`
<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)
Domain Name: 15hotel.cn
ROID: 20201230s10001s33844513-cn
Domain Status: ok

Registrant: 刘芳 [Liu Fang]
Registrant Contact Email: zhang73983chen139@163.com

Sponsoring Registrar: 阿里巴巴云·算(北京)有限公司 [Alibaba Cloud Computing (Beijing) Co., Ltd.]

Registration Time: 2020-12-30 20:18:59
Expiration Time: 2021-12-30 20:18:59

Name Server: harley.ns.cloudflare.com
Name Server: sierra.ns.cloudflare.com

DNSSEC: unsigned
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>cbvkia[.]bar</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.138.43, 104.21.64.240</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:** CBVKIA.BAR  
**Registry Domain ID:** D221899058-CNIC  
**Registrar WHOIS Server:** whois.rrpproxy.net  
**Registrar URL:** http://www.key-systems.net  
**Registrar:** Key-Systems LLC  
**Registrar IANA ID:** 1345  

**Updated Date:** 2021-07-20T06:35:55.0Z  
**Creation Date:** 2021-02-16T15:11:59.0Z  
**Registry Expiry Date:** 2022-02-16T23:59:59.0Z  

**Registrar:** Key-Systems LLC  
**Registrar IANA ID:** 1345  

**Registrant Country:** CN (China)  

**Name Server:** GORDON.NS.CLOUDFLARE.COM  
HOPE.NS.CLOUDFLARE.COM
Conclusive Summary:

- The campaign is pretended to be an offer from Flipkart but hosted on the third party domain instead of the official website of Flipkart 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 prizes are kept really attractive to lure the laymen.
- The campaign collects browser and system information from the users.
- 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 Flipkart 15th Anniversary free gifts 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 should 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 compromisation (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.