OSINT Report on

“Big Billion Days Spin The Lucky Wheel!” scam
OSINT Report on
“Big Billion Days Spin The Lucky Wheel!” scam:

The Research Wing at CyberPeace Foundation has received some links via Whatsapp related to Big Billion Days pretending to be an offer from Amazon.

Forwarded

[Amazon logo]
Big Billion Days 🎉
See how lucky you are!
gift23.xyz

https://gift23.xyz/j/?c=spin

13:03:41

Forwarded

[Amazon logo]
Big Billion Days 🎉
See how lucky you are!
vip-j4.work

https://vip-j4.work/j/?c=sp

2:37 pm

Case Study:

The link https://gift23[.]xyz/j/?c=spin redirects to https://free35[.]xyz/spin/#XX and the link https://vip-j4[.]work/j/?c=sp redirects to https://vip-l43.work/sp/?th=#XX

** where XX represents unique 13 digits number, for example #1607324988200, #1607325659000 etc.

On the landing page a lucky draw spinning wheel can be seen, on clicking the SPIN button it shows ‘You Won 1 Free Extra Spin!’ with an alert.
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 much the offer is beneficial.

On the second try on the SPIN button it shows an alert based message:

"Congratulations! Your prize: OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage). Please follow the instructions to win your prize!" and clicking on the OK button of the alert message it shows a section which contains a congratulations message with the details of the product which users have owned.

Also it instructs users to share the campaign on Whatsapp.
After clicking on the green Whatsapp button multiple times it shows a section where an instruction has been given to download an application in order to get the prize.

![Congratulations! The last step:](image)

After clicking on the green **Download App** button it redirects the user to a link `https://goraps[.]com/fullpage.php?section=General&pub=382565&ga=g`.

**In Depth Investigation:**

The Research Wing at CyberPeace Foundation along with Autobot Infosec Private Limited have looked forward to this matter to come to a conclusion that these websites are either legitimate or an online fraud. Some key findings can be mentioned as:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>gift23[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Status Code</strong></td>
<td>200 [Active]</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>172.67.194.41, 104.27.174.129, 104.27.175.129</td>
</tr>
<tr>
<td><strong>ISP</strong></td>
<td>Cloudflare</td>
</tr>
<tr>
<td><strong>ASN</strong></td>
<td>13335</td>
</tr>
<tr>
<td><strong>Country</strong></td>
<td>United States 🇺🇸</td>
</tr>
<tr>
<td><strong>Continent</strong></td>
<td>North America</td>
</tr>
</tbody>
</table>
Registry Domain ID: D212862963-CNIC
Registrar WHOIS Server: grs-whois.hichina.com

Updated Date: 2020-12-04T18:36:30.0Z
Creation Date: 2020-12-04T18:26:10.0Z
Registry Expiry Date: 2021-12-04T23:59:59.0Z

Registrar: Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
Registrar IANA ID: 1599

Registrant Organization: fang xiao qing
Registrant State/Province: guang dong
Registrant Country: CN (China)

Name Servers: LIBERTY.NS.CLOUDFLARE.COM
              TODD.NS.CLOUDFLARE.COM

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>free35[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.165.128, 104.24.114.224, 104.24.115.224</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>

Registry Domain ID: D213052838-CNIC
Registrar WHOIS Server: grs-whois.hichina.com

Updated Date: 2020-12-07T00:13:38.0Z
Creation Date: 2020-12-07T00:02:14.0Z
Registry Expiry Date: 2021-12-07T23:59:59.0Z
Registrar: Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
Registrar IANA ID: 1599

Registrant Organization: fang xiao qing
Registrant State/Province: guang dong
Registrant Country: CN (China)

Name Servers: JOSELYN.NS.CLOUDFLARE.COM
YEW.NS.CLOUDFLARE.COM

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>vip-j4[.]work</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>35.205.100.210</td>
</tr>
<tr>
<td>ISP</td>
<td>Google Cloud</td>
</tr>
<tr>
<td>ASN</td>
<td>15169</td>
</tr>
<tr>
<td>Country</td>
<td>Belgium</td>
</tr>
<tr>
<td>Continent</td>
<td>Europe</td>
</tr>
</tbody>
</table>

Registry Domain ID:
D_01E2B629_505DE4EA498D47A2B32CEE1A66E850B8_00000176230398FC-WORK
Creation Date: 2020-12-02T10:33:27Z
Registry Expiry Date: 2021-12-02T10:33:27Z
Registrar: ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
Registrar IANA ID: 3775
Registrar Abuse Contact Email: abuse@list.alibaba-inc.com
Registrar Abuse Contact Phone: +86.10659859

Registrant State/Province: he nan
Registrant Country: CN (China)

Name Servers: ns7.alidns.com
ns8.alidns.com
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>vip-l43[.]work</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.31.83.142, 104.31.82.142, 172.67.190.38</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>

Registry Domain ID:
D_01E33404_14517B4346754EECAB8C8204CDB84C80_0000017638CBB357-WORK

Updated Date: 2020-12-06T16:11:36Z
Creation Date: 2020-12-06T16:04:02Z
Registry Expiry Date: 2021-12-06T16:04:02Z
Registrar: ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
Registrar IANA ID: 3775
Registrar Abuse Contact Email: abuse@list.alibaba-inc.com
Registrar Abuse Contact Phone: +86.10659859

Registrant State/Province: he nan
Registrant Country: CN

Name Server: adaline.ns.cloudflare.com
              vicky.ns.cloudflare.com
HTTP Header Response:

https://free33[.]xyz/spin/#1607411105900

<table>
<thead>
<tr>
<th>HTTP/1.1 200 OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>Content-Type:</td>
</tr>
<tr>
<td>Transfer-Encoding:</td>
</tr>
<tr>
<td>Connection:</td>
</tr>
<tr>
<td>Set-Cookie:</td>
</tr>
<tr>
<td>Vary:</td>
</tr>
<tr>
<td>CF-Cache-Status:</td>
</tr>
<tr>
<td>cf-request-id:</td>
</tr>
<tr>
<td>Report-To:</td>
</tr>
<tr>
<td>NEL:</td>
</tr>
<tr>
<td>Server:</td>
</tr>
<tr>
<td>CF-RAY:</td>
</tr>
</tbody>
</table>
In source code analysis we found some information like --

- Title of the site is **Big Billion Days**.
  
- The title image pretending to be the brand of Amazon is hosted on Imgur [https://i.imgur[.]com/fw0ig00.png](https://i.imgur[.]com/fw0ig00.png).
Reverse image search on the above image gives the result -

- The section which seems to be a Facebook comment area is a static, not a dynamic one. The section has been created with some HTML and CSS. Everytime the website has been visited, the section remains the same. Time of the comments always remains the same like 1 hour ago and 29 minutes ago.

Piece of HTML code for fake Facebook comment section

```
</div>
</div>
</div>

Piece of CSS codes for fake Facebook comment section

```
The Profile pictures for the comments are linked with the images hosted in blogspot.

The link of the profile images are --

1) https://i.imgur[.]com/k51iY1s.jpg
2) https://i.imgur[.]com/gg3teDe.jpg
3) https://i.imgur[.]com/jXhB4c6.jpg
4) https://i.imgur[.]com/1H2Gelw.jpg
5) https://i.imgur[.]com/IhePd0v.jpg
6) https://i.imgur[.]com/AAKwzHS.jpg
7) https://i.imgur[.]com/SMfvBNU.jpg
8) https://i.imgur[.]com/sQZsRZH.jpg
9) https://i.imgur[.]com/T5yM1yR.jpg
10) https://i.imgur[.]com/rWJaWux.jpg
11) https://i.imgur[.]com/wYUu4Np.jpg
12) https://i.imgur[.]com/aM50FsF.jpg

We have done reverse image investigation on the images and found that some of the images have been used multiple times on the same type of campaign. One of the images has been used for call girl service.
From the piece of code written in javascript it is proved that users can win only **OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage)** whereas many other products are pretended to be owned on the wheel.

**Piece of JS code to lure users to win OPPO F17 Pro**

- Users are insisted to share the campaign with Whatsapp friends and groups.

**Piece of JS code to insist user to share on Whatsapp**
Google tag manager id found G-Y6JD8EYCMPP and UA-174943768-7 for https://free35.xyz/spin/#XX and https://vip-l43[.]work/sp/?th=#XX respectively.


Some other links found --

http://www.w3.org/1999/xlink
http://www.w3.org/2000/svg
https://amazon.com
https://gkjw.getyouritem.net/c/1f0a2cb367c37dee?s1=72530&s2=1147389&j1=1&j3=1&click_id=MTA1OC01NTY5&s3=10004&s5=1058
https://gkjw.getyouritem.net/c/1f0a2cb367c37dee?s1=72530&s2=1147389&j1=1&j3=1&click_id=MTA1OS03Mjk3&s3=10004&s5=1059
https://goraps.com/fulpage.php?section=spfin&pub=989147&ga=g
https://hm.baidu.com/hm.js?c69539a227ba2e3ff7b088a31ae442be
https://uprimp.com/bnr.php?section=spb&pub=989147&format=300x50&ga=g

The redirected link
https://goraps[.]com/fulpage.php?section=General&pub=382565&ga=g (This link is a ylliX Inc link. ylliX Inc is an advertiser company) ultimately redirects to http://www.ttyuki[.]cn/ which is a Chinese hosting company
One thing to be mentioned here is that the url redirects users randomly to multiple sites.

**Conclusions:**

- The Big Billion Days campaign is being pretended to be an offer from Amazon but actually the Big Billion days is an offer from Flipkart.

- Grammatical mistakes have been found on the webpage, any big brand organisation usually does not have any grammatical mistakes.

- From the piece of code written in javascript it is proved that users can own only OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage) whereas many other products are pretended to be owned on the wheel.

- The domains have been registered from China.

**Issued by:**

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