Research Report on

“Year-end carnival Get free Christmas gifts!” scam
Research Report on “Year-end carnival Get free Christmas gifts!” scam

The Research Wing at CyberPeace Foundation has come across some links via Whatsapp related to Year-end carnival pretending to be an offer from Flipkart.

Case Study:

The link https://xngmibi[].top/lhj/?i=en&x=1&t=19 redirects to https://ozf-whatsapp[].xyz/lh-j/l.php?l=en&x=1&t=21#XX, the link https://vnrgjms[].top/lhj/?i=en&x=1&t=19 and https://ngddww-f[].top/lhj/?i=en&x=1&t=21 redirect to https://uwm-whatsapp[].xyz/lhj/l.php?l=en&x=1&t=21#XX

** Where XX represents unique 13 digits number, for example #1608534552200 and #1608543495500

On the landing page a lucky draw section can be seen, on clicking the start button it shows ‘It’s a pity that you didn’t get the reward, you have 2 more chances’ 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.

Clicking on the Ok button of the alert it starts the lucky draw again and shows an alert "It's a pity that you didn't get the reward, you have 1 more chance"

On the third try it shows an alert based message: "Congratulations! Your prize: OPPO F17 Pro (Matte Black, 86GB 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 with 5 groups / 20 friends on Whatsapp.
After clicking on the green WhatsApp button multiple times (until the blue progress bar ends) it shows a section where an instruction has been given to download an application in order to get the prize.

**Congratulations!**

You have won **OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage)**. We’ve only 13 OPPOF17 Pro left for this week. Follow the instructions below in order to claim your OPPO F17 Pro.

**Congratulations! The last step:**

You have to complete this final step!

1. You have to install the application below and once installed you have to open it for 30 seconds.
   (Remember, this step is very important)

After completing the above actions, please wait for admin to check it, the review will be completed within 24 hours.

Everytime user clicks on the WhatsApp button a new tab opens on browser with the link

```plaintext
whatsapp://send?text= https%3A%2F%2Fpktnoxl.top%2Flhj%2F%3F%3Den%26x%3D1%26t%3D21
```

It means if the user clicks on the link from a mobile device it will open the installed WhatsApp application on the phone.

We have also noticed an alert message like "**Sharing failed!The same group or the same friend is not correct. Please check and share again.**"

After clicking on the green **Download App** button it redirects the user to a link

```plaintext
https://mavq[.]net/7f84645690/2d1d099658/?placementName=default
```
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><strong>Domain Name</strong></th>
<th>xngmibi[.]top</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>172.67.217.189, 104.31.89.25, 104.31.88.25</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:** D2020113G10001G_51591769-top  
**Registrar WHOIS Server:** whois.hichina.com  
**Updated Date:** 2020-12-16T02:23:46Z  
**Creation Date:** 2020-11-13T04:17:11Z  
**Registry Expiry Date:** 2021-11-13T04:17:11Z  

**Registrar:** Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)  
**Registrar IANA ID:** 1599  
**Registrar Abuse Contact Email:** DomainAbuse@service.aliyun.com  
**Registrar Abuse Contact Phone:** +86.95187

**Registrant Organization:** yu guang chao  
**Registrant State/Province:** guang dong  
**Registrant Country:** CN (China)
Domain Name | ozf-whatsapp[.]xyz
---|---
HTTP Status Code | 200 [ Active ]
IP Address | 104.27.179.140, 172.67.191.141, 104.27.178.140
ISP | Cloudflare
ASN | 13335
Country | United States 🇺🇸
Continent | North America

Registry Domain ID: D213201773-CNIC
Registrar WHOIS Server: grs-whois.hichina.com

Creation Date: 2020-12-08T08:00:16.0Z
Registry Expiry Date: 2021-12-08T23:59:59.0Z

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

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

Name Servers: AMIR.NS.CLOUDFLARE.COM
MIKI.NS.CLOUDFLARE.COM

DNSSEC: unsigned
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>vnrgjms[.]top</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.27.173.70, 172.67.208.173, 104.27.172.70</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:** D20201112G10001G_51539673-top  
**Registrar WHOIS Server:** whois.hichina.com  
**Registrar URL:** http://www.net.cn  

**Updated Date:** 2020-12-16T02:51:05Z  
**Creation Date:** 2020-11-12T05:09:33Z  
**Registry Expiry Date:** 2021-11-12T05:09:33Z  

**Registrar:** Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)  
**Registrar IANA ID:** 1599  
**Registrar Abuse Contact Email:** DomainAbuse@service.aliyun.com  
**Registrar Abuse Contact Phone:** +86.95187  

**Registrant Organization:** yu guang chao  
**Registrant State/Province:** guang dong  
**Registrant Country:** CN (China)  

**Name Servers:** amir.ns.cloudflare.com  
                      miki.ns.cloudflare.com  

**DNSSEC:** unsigned
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>ngddwwf[.]top</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.201.222, 104.27.178.97, 104.27.179.97</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:** D20201112G10001G_51540401-top  
**Registrar WHOIS Server:** whois.hichina.com  
**Registrar URL:** http://www.net.cn  
**Updated Date:** 2020-12-16T02:51:05Z  
**Creation Date:** 2020-11-12T05:27:19Z  
**Registry Expiry Date:** 2021-11-12T05:27:19Z  

**Registrar:** Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)  
**Registrar IANA ID:** 1599  
**Registrar Abuse Contact Email:** DomainAbuse@service.aliyun.com  
**Registrar Abuse Contact Phone:** +86.95187  

**Registrant Organization:** yu guang chao  
**Registrant State/Province:** guang dong  
**Registrant Country:** CN (China)  

**Name Servers:** amir.ns.cloudflare.com  
                    miki.ns.cloudflare.com  

**DNSSEC:** unsigned
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>uwm-whatsapp[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.24.117.69, 104.24.116.69, 172.67.208.4</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: D213202008-CNIC
Registrar WHOIS Server: grs-whois.hichina.com

Creation Date: 2020-12-08T08:00:58.0Z
Registry Expiry Date: 2021-12-08T23:59:59.0Z

Registrar: Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
Registrar IANA ID: 1599
Registrar Abuse Contact Email: domainabuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187

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

Name Servers: AMIR.NS.CLOUDFLARE.COM
               MIKI.NS.CLOUDFLARE.COM

DNSSEC: unsigned
HTTP Header Response:

https://ozf-whatsapp[.]xyz/lhj/l.php?!en&x=1&t=21#1608534552200

<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>Access-Control-Allow-Origin:</td>
</tr>
<tr>
<td>Strict-Transport-Security:</td>
</tr>
<tr>
<td>Z-Server:</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>
HTTP/1.1 200 OK
Date: Tue, 22 Dec 2020 16:18:58 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: __cfduid=d45da221dfb5c9e3347cbca61cc6e4f9b1608653938; expires=Thu, 21-Jan-21 16:18:58 GMT; path=/; domain=.uwm-whatsapp.xyz; HttpOnly; SameSite=Lax; Secure
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Strict-Transport-Security: max-age=31536000
Z-Server: 10.168.0.2
CF-Cache-Status: DYNAMIC
cf-request-id: 072cd8358200000740999096000000001
Report-To: ["endpoints":[{"url":"https://a.nel.cloudflare.com/vreport/s=pAQhFSe7vkk7u6aUJShCThn9mzLTRofNHUNrkyYmH6YDh1P2DFfbtP0N2Cl0W%2FD%2F%2F4XmU2gQGTP18w35sqRcRW2Xk6usozDrCyO5EG8vIq%2F"}],"group":"cf-nel","max_age":604800}]
NEL: ["report_to":"cf-nel","max_age":604800]
In source code analysis we found some information like --

- Titles of the sites are Year-end carnival.
- The title image pretending to be the brand of Flipkart is hosted on blogspot. https://1.bp.blogspot[-NJ4N25s/X9xcitc-UbCl/AAAAAAXAAAgA/xo9_LHjSTBQ0Ej8alN3c3tuR_pB2t-l_gCLcBGAyYQ/s0/Flipkart.jpg

- 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.

```html
<p class="totlikes">Priyanka Kapoor: Last week I played and won OPPO F17 Pro and guess what? I've received my phone. I'm loving it.</p>
</div>
</div>
</div>
</div>
</div>
</div>
</div>

Piece of HTML code for fake Facebook comment section

```css
.totlikes {
  margin-top: 3px;
  background-color: #eef4f4;
  padding: 5px 5px 5px 23px;
  background-repeat: no-repeat;
  background-position: 5px center;
}

.fblike {
  color: #3c5a96;
  font-size: 0.95em;
  cursor: pointer;
}

.fblike:hover {
  text-decoration: underline;
}
```

Piece of CSS codes for fake Facebook comment section
The Profile pictures for the comments are linked with the images hosted on imgur.

The link of the profile images are --

1. https://i.imgur[]com/k51iYIs.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/lhePdoV.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 noticed that the profile images are the same images that were used in “Big Billion Days Spin The Lucky Wheel” scam. On reverse image investigation we found images have been used on many same types of scam.
We have noticed that every time a user wins the **OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage)** only, whereas many other products are pretended to be owned on the lucky draw. Here are some pieces of Javascript code extracted from the source code.

```
settings.zj_arr.is_win=0;
$$('#game3').find('.game-goods-ul').on(‘webkitTransitionEnd’, function() {
    if(times==1){
        alert("It’s a pity that you didn’t get the reward, you have 2 more chances");
    }else{
        alert("It’s a pity that you didn’t get the reward, you have 1 more chance");
    }
    setTimeout(function(){beginGame();}, 100);
});

setTimeout(function(){
    if(!haveWinPrompt){
        stopConfetti();
        haveWinPrompt = true;
        e = alert("Congratulations! Your prize: OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage). Please follow the instructions to win your prize!");
        e === 10 || $('.hide all').hide(), $('.show all').show();
        $('body').css({'overflow':'initial'});
        $('body').css({'position':'relative'});
    }, 4000);
}
```

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

We have found comment written in chinese language in the source code of the site.

```
var times=0;

//测试请删掉
set_cookie('iszj',0);

$.extend({
    //
});
```

Comment found written in Chinese language
• Google tag manager id found G-C7JY0WBZK5 for both sites https://ozf-whatsapp[.]xyz/lhj/l.php?l=en&x=1&t=21#XX and https://uwm-whatsapp[.]xyz/lhj/l.php?l=en&x=1&t=21#XX

• www.googletagmanager[.]com/gtag/js?id=G-C7JY0WBZK5

• Some other links found --

http://www.w3.org/1999/xlink
http://www.w3.org/2000/svg
https://cdn.jsdelivr.net/npm/lazyload@2.0.0-rc.2/lazyload.js
https://cdnjs.cloudflare.com/ajax/libs/bootstrap-sweetalert/1.0.1/sweetalert.min.css
https://cdnjs.cloudflare.com/ajax/libs/bootstrap-sweetalert/1.0.1/sweetalert.min.js
https://cukqeyi.top/lhj/?l=en&x=1&t=23
https://cukqeyi.top/lhjj/?x=1
https://stackpath.bootstrapcdncdn.com/bootstrap/4.1.3/css/bootstrap.min.css
https://uprimp.com/bnr.php?section=General&pub=518855&format=300x50&ga=g

In our case the redirected link https://mavq[.]net/7f84645690/2d1d099658/?placementName=default ultimately redirects to https://planettravel[.]net/lp.php?cc=-&hash=affC1608541570aff6d2fb04637759a493a35 (Which is a travel booking website) but one thing to be noted is that the url https://mavq[.]net/7f84645690/2d1d099658/?placementName=default redirects to other random sites also.
Conclusions:

- Flipkart Year end carnival was announced for the month of December 2018. In 2020 we did not find any information on flipkart official website regarding Year end carnival.
- Grammatical mistakes have been found on the webpage, any big brand organisation usually does not have any grammatical mistakes.
- Usually any big brand ecommerce entity holds any offer on their respective official website. The offer is hosted on some suspicious websites instead of the official website https://flipkart.com.
- The owner of the sites that are being shared via social media platform, is not Flipkart Internet Private Limited. On the basis of our investigation and extracted information, it seems that the sites are registered from the region of China.

Issued by:

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