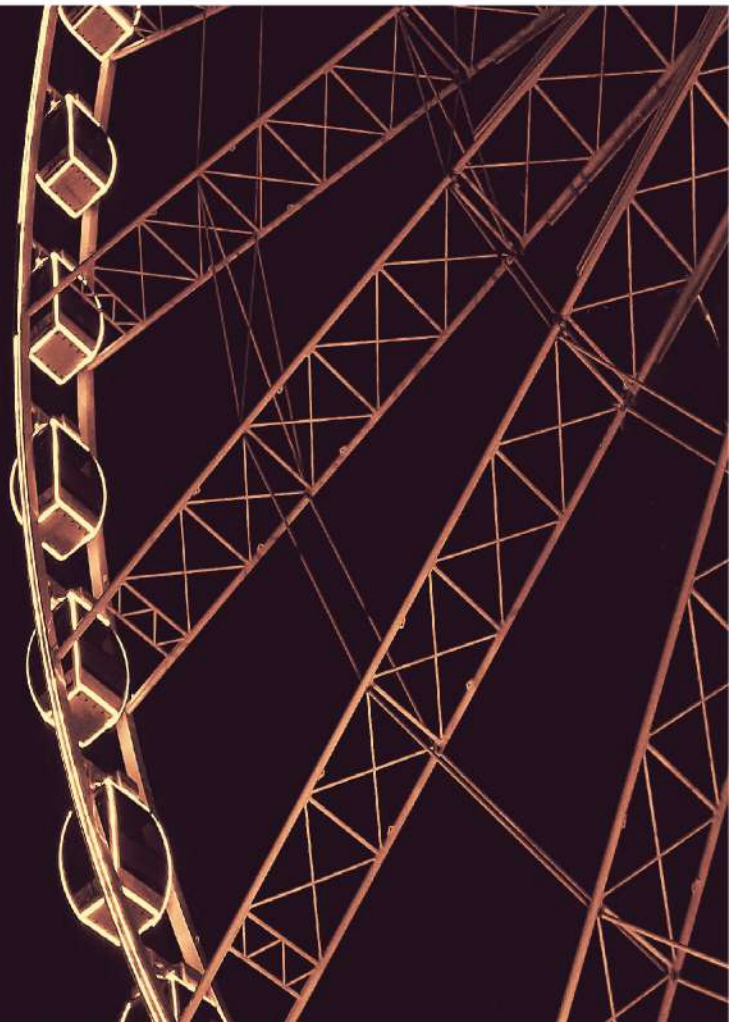
CyberPeace
Foundation

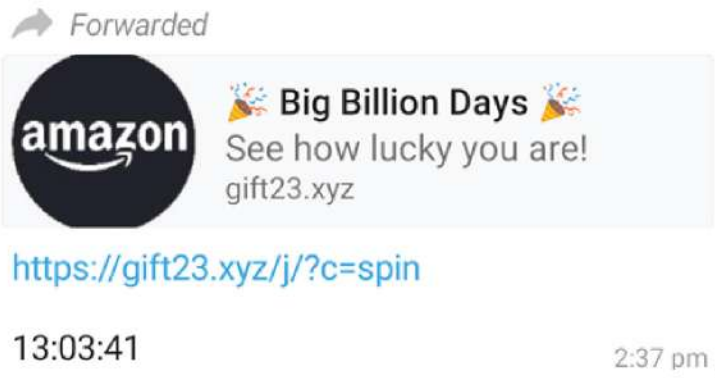
OSINT Report on

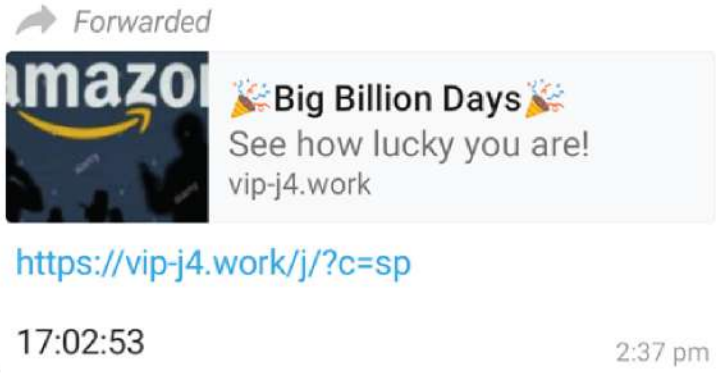
“Big Billion Days Spin The Lucky Wheel!” scam



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.



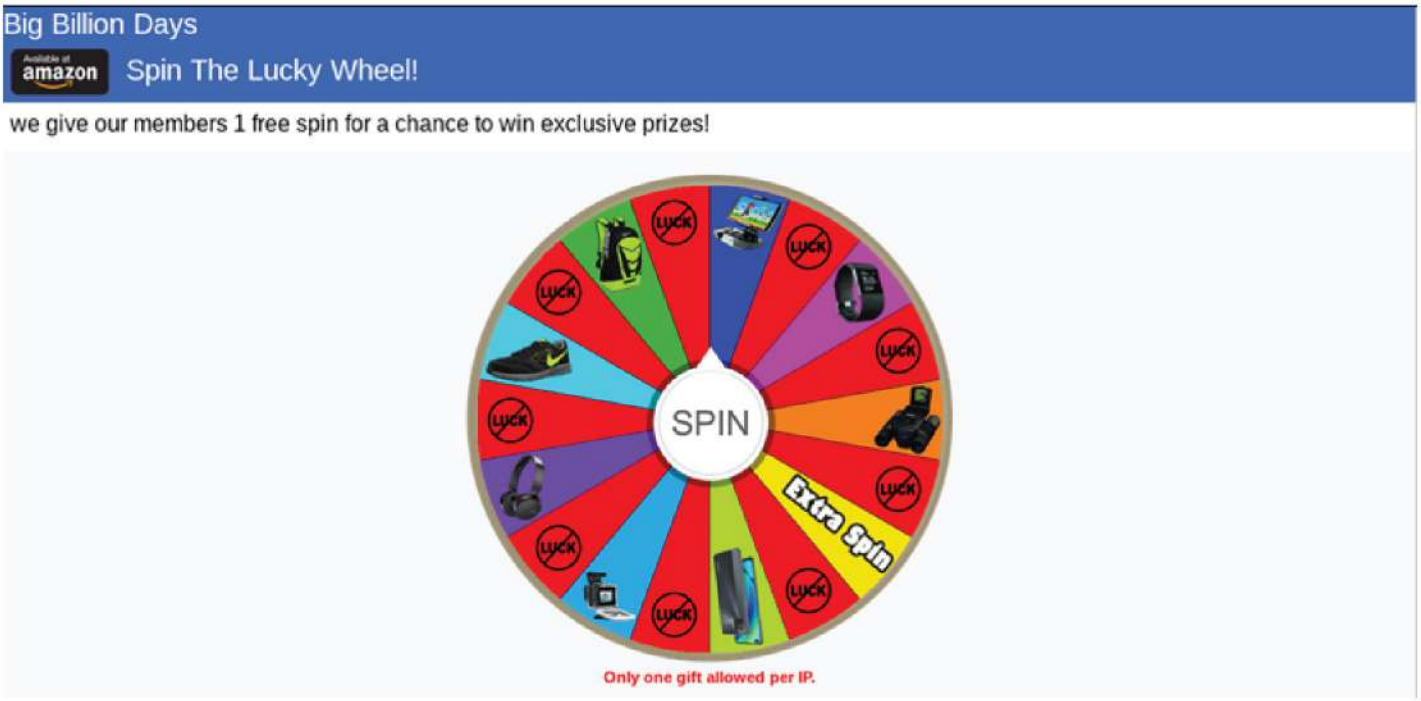


Case Study:

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

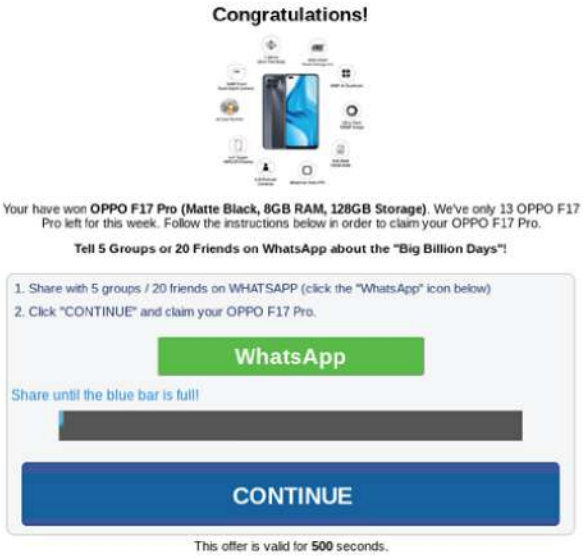
** where XX represents unique 13 digits number, for example #1607324988200, #1607325659000 etc.

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.

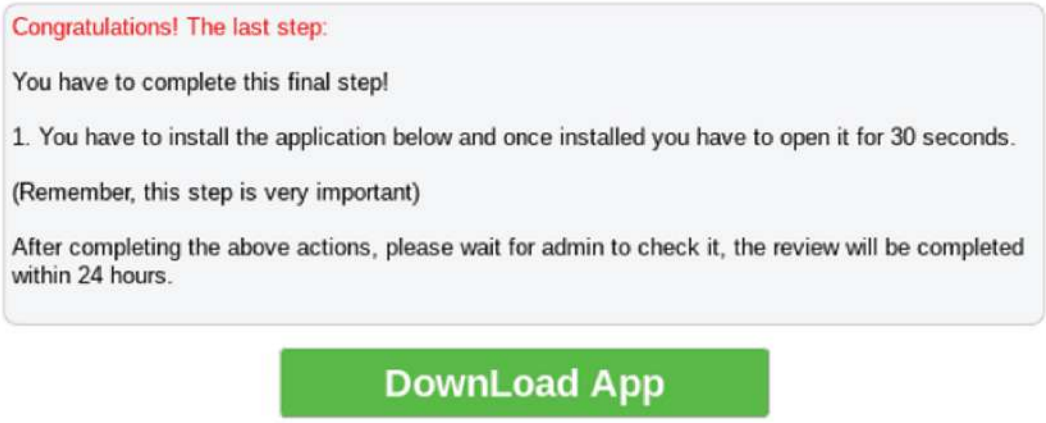
On the second try on the SPIN button it shows an alert based message :



'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.



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--

Domain Name	**gift23[.]xyz**
HTTP Status Code	**200 [Active]**
IP Address	172.67.194.41, 104.27.174.129, 104.27.175.129
ISP	Cloudflare
ASN	13335
Country	United States
Continent	North America

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

Domain Name	free35[.]xyz
HTTP Status Code	200 [Active]
IP Address	172.67.165.128, 104.24.114.224, 104.24.115.224
ISP	Cloudflare
ASN	13335
Country	United States
Continent	North America

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

Domain Name	vip-j4[.]work
HTTP Status Code	200 [Active]
IP Address	35.205.100.210
ISP	Google Cloud
ASN	15169
Country	Belgium
Continent	Europe

Registry Domain ID:
D_01E28629_506DE4EA498D47A2B32CEE1A66E850B8_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

Domain Name	vip-l43[.]work
HTTP Status Code	200 [Active]
IP Address	104.31.83.142,104.31.82.142, 172.67.190.38
ISP	Cloudflare
ASN	13335
Country	United States
Continent	North America

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

HTTP/1.1 200 OK	
Date:	Tue, 08 Dec 2020 07:23:57 GMT
Content-Type:	text/html; charset=UTF-8
Transfer-Encoding:	chunked
Connection:	close
Set-Cookie:	__cfduid=d03d1aa8b421c5bd1b258bef0721f5f721607412237; expires=Thu, 07-Jan-21 07:23:57 GMT; path=/; domain=.free33.xyz; HttpOnly; SameSite=Lax
Vary:	Accept-Encoding
CF-Cache-Status:	DYNAMIC
cf-request-id:	06e2d55e130000386bda2d0000000001
Expect-CT:	max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=8PIMDE7uV6RR%2FCw6SHNTaQb03g4cdJ3ck6JAeKULEsZjVc%2BTodgJG0CBPB3xaoh2XliqonPj5B74SugHBrQp3cywCPvA1D4WTUU5"}],"group":"cf-nel","max_age":604800}
NEL:	{"report_to":"cf-nel","max_age":604800}
Server:	cloudflare
CF-RAY:	5fe4be7689f6386b-IAD

https://vip-l43[.]work/sp/?th=#1607411409200

HTTP/1.1 200 OK	
Date:	Tue, 08 Dec 2020 07:28:44 GMT
Content-Type:	text/html; charset=UTF-8
Transfer-Encoding:	chunked
Connection:	close
Set-Cookie:	__cfduid=df80b671314fff0d5cdc3f11a9ed4e1b91607412524; expires=Thu, 07-Jan-21 07:28:44 GMT; path=/; domain=.vip-l43.work; HttpOnly; SameSite=Lax
Vary:	Accept-Encoding
CF-Cache-Status:	DYNAMIC
cf-request-id:	06e2d9be8500002aec39b3a000000001
Expect-CT:	max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:	{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=82JxfWvffWW5IPTw189PqL3o2QFM%2FliquVxj8nWxaqQXGt%2BWAxCstu%2BVVV8yGxhni2z4CFUtvQuk4bsJov6bPbEBbvRz1YSqTuI7p6U%3D"}],"group":"cf-nel","max_age":604800}
NEL:	{"report_to":"cf-nel","max_age":604800}
Server:	cloudflare
CF-RAY:	5fe4c5773d132aec-IAD

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/fwQig0O.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.

```
<p class="totlikes"><span id="youand"></span><span class="fbblue">12,068 others</span> like this</p>
<p class="viewmore clearfix">
    <span class="left">View more comments</span>
    <span class="right">15 of 1,356</span>
</p>
<div class="item">
    <img class="profileimg" src="https://i.imgur.com/k51iYls.jpg" height="50" width="50">
    <p class="comtxt"><span class="name">Priyanka Kapoor</span> yeahhhhh.. Last week I played and won OPPO F17 Pro  and
        guess what?? Today I've received my phone. I am loving it. </p>
    <p class="combot"><span class="ago">4 minutes ago</span> <span class="fblike">Like</span><span class="likes totlikes">37
        </span></p>
</div>
<div class="item">
    <img class="profileimg" src="https://i.imgur.com/gg3teDe.jpg" height="50" width="50">
    <p class="comtxt"><span class="name">Prashik Suntakke</span> I got the bagpack.. Thanks Thankssss.. This is the best day
        ever  ..</p>
    <p class="combot"><span class="ago">13 minutes ago</span> <span class="fblike">Like</span><span class="likes totlikes">24
        </span></p>
</div>
<div class="item">
    <img class="profileimg" src="https://i.imgur.com/jXhB4c6.jpg" height="50" width="50">
    <p class="comtxt"><span class="name">Prakash Panwar</span> Amazing game. Just found it. Hope I will win. EDIT: I got
        nothing </p>
    <p class="combot"><span class="ago">29 minutes ago</span> <span class="fblike">Like</span><span class="likes totlikes">14
        </span></p>
</div>
```

Piece of HTML code for fake Facebook comment section

```
.totlikes {
    margin-top: 3px;
    background-color: #eeeff4;
    padding: 5px 5px 5px 23px;
    background-repeat: no-repeat;
    background-position: 5px center
}
```

```
.fblike {
    color: #3c5a96;
    font-size: .95em;
    cursor: pointer
}

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

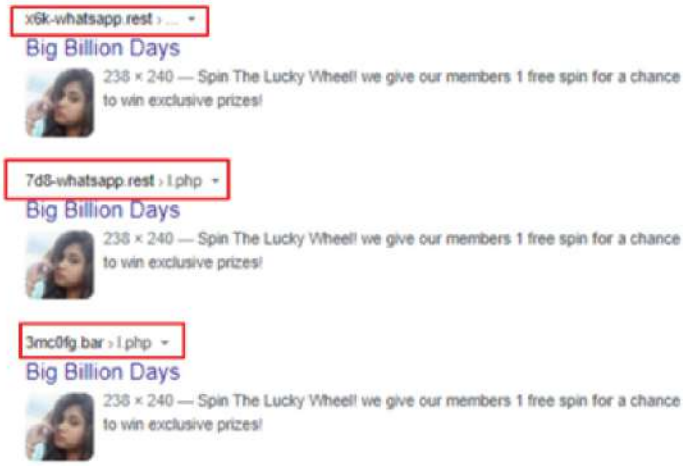
Piece of CSS codes for fake Facebook comment section

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

The link of the profile images are --

1) *https://i.imgur[.]com/k51iYls.jpg*
2) *https://i.imgur[.]com/gg3teDe.jpg*
3) *https://i.imgur[.]com/jXhB4c6.jpg*
4) *https://i.imgur[.]com/1H2GeIw.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.

```
function startSpin() {
    var e = document.getElementById("spin"),
        n = document.getElementById("win"),
        t = document.getElementById("winP"),
        o = document.getElementById("win2");
    e.className = e.className + "spinAround", n.style.display = "none", t.style.display = "block", setTimeout(function() {
        t.style.display = "none", o.style.display = "block"
    }, 150), setTimeout(function() {
        alert("You Won 1 Free Extra Spin!"), spin2enabled = !0
    }, 6500)
}

function spin2() {
    if (spin2enabled) {
        var e = document.getElementById("spin"),
            n = document.getElementById("win"),
            t = document.getElementById("winP"),
            o = document.getElementById("win2");
        e.className = e.className + " spinAround2", n.style.display = "none", t.style.display = "block", setTimeout(
            function() {
                t.style.display = "none", o.style.display = "block"
            }, 150), setTimeout(function() {
            var e = alert(
                "Congratulations!\n\nYour prize: OPPO F17 Pro (Matte Black, 8GB RAM, 128GB Storage).\n\nPlease follow the
                    instructions to win your prize!"
            );
            e === !0 || $(".hide-all").hide(), $(".show-all").show();
        }, 6800)
    }
}
```

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

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

```
function incrementValue1() {
    if (parseInt(get_Cookie('prog')) > 200) {
        // window.open('whatsapp://send?text=' + tb);
        location.href='whatsapp://send?text=' + tb;
    } else {
        // window.open('whatsapp://send?text=' + tb);
        location.href='whatsapp://send?text=' + tb;
    }
    setTimeout(function() {

        incrementValue_i();
        fn1_i();
        value = parseInt(get_Cookie('prog'));
        set_Cookie('prog', value + 1);
    }, 2000);
}

function incrementValue_i() {
    get_Cookie('prog') == '' ? value = 0 : value = get_Cookie('prog');
    value == 2 || value == 4 ? alert(
        'Sharing failed!\n\n The same group or the same friend is not correct. Please check and share again.') : void(0);
    set_Cookie('prog', value);
    if (value >= 12) {
        lasthtml();
    }
}
```

Piece of JS code to insist user to share on Whatsapp

Google tag manager id found **G-Y6JD8EYCMP** and **UA-174943768-7** for **https://free35[.]xyz/spin/#XX and https://vip-l43[.]work/sp/?th=#XX** respectively.

• https://www.googletagmanager.com/gtag/js?id=G-Y6JD8EYCMP

• https://www.googletagmanager.com/gtag/js?id=UA-174943768-7

Some other links found --

http://www.w3.org/1999/xlink
http://www.w3.org/2000/svg
https://amazon.com
https://gkjow.getyouritem.net/c/1f0a2cb367c37dee?s1=72530&s2=1147389&j1=1&j3=1&click_id=MTA1OC01NTY5&s3=10004&s5=1058
https://gkjow.getyouritem.net/c/1f0a2cb367c37dee?s1=72530&s2=1147389&j1=1&j3=1&click_id=MTA1OS03Mjk3&s3=10004&s5=1059
https://goraps.com/fullpage.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/fullpage.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.

CyberPeace
Foundation

www.cyberpeace.org | secretariat@cyberpeace.net


/cyberpeacefoundation

/cyberpeacengo

/cyberpeacefoundation