RESEARCH REPORT ON:

‘Free Women’s Day Gift’ 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, information might be changed after generating the reports.
Research report on ‘Free Women’s Day Gift’ scam:

The Research Wing of CyberPeace Foundation received some links via WhatsApp related to a Women’s Day gift pretending to be an offer from reputed companies like Amazon, Adidas, and TATA.

Case Study:

**Gift from Amazon:** On visiting the link https://oovip[.]xyz/hw/?v=20210205 it redirects users to https://phonesvip[.]xyz/hw/luodi.php#XX

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

On the landing page a popup opened with an offer detail.

“🎁 Women’s Day Gift❤️

More than 1000 units of chocolate and mobile equipment, as well as 500 cash prizes ranging from 50 to 5000 US dollars. All you have to do is open the correct gift box.

You have 3 tries, good luck!”
After clicking on the ‘OK’ button it asks users to participate in a quick survey to get free Women’s Day Gifts from Amazon.

Clicking on the ‘Start here’ button the survey starts with some basic questions like “Do you know amazon?, Which social software do you use more often?, Which amazon product do you want to buy as a Women’s Day gift??” etc.
On completing the survey it says that the user is eligible to open the gift box.

After that the user is given three attempts to win the prize.

After completing all the attempts it says that the user has won ‘**Huawei Mate 40 Pro 5G Full Netcom 8GB + 256GB (bright black)**’.

**“CONGRATULATIONS! You guessed! Your prize money is: Huawei Mate 40 Pro 5G Full Netcom 8GB + 256GB (bright black). Follow the instructions on the next page to claim your prize!”**

In between each attempt it shows some message which says how many attempts are left.
Clicking on the 'OK' button 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 complete registration in order to get the prize.
After clicking on the green 'Complete registration' button, it redirects the user to a link https://www.graburprize[.]net/c/b795ebb3cf6XXXXX?&click_id=XXXXX&s1=72530&s2=1238468&s3=backuser&s5=&lp=MJ&j4=&j5=&j6= where another loyalty program with spin the wheel can be seen.

**[Some characters are replaced with XX for security reasons.]**

Also, at the bottom of this page a section comes up which seems to be a social media comment section where many users have commented about how the offer is beneficial.
Users can spin the wheel 2 times and after completion it shows another congratulations message with two options to choose.

During the investigation we noticed whichever option is chosen it redirects to the same Loyalty program page again.

**Gift from Adidas**: For the second link [https://v-app[]buzz/adidas/tb.php?_t=1614915696](https://v-app[]buzz/adidas/tb.php?_t=1614915696) it also lures the laymen to get into the offer similar to the first one. Instead of the **Huawei** phone in this case **Adidas ‘SUPERSTAR’** is kept as a gift.

After asking to share the campaign on WhatsApp, it takes users to the same type of spin the wheel loyalty program page discussed earlier.
**Gift from TATA:** During the investigation we noticed the link [https://tatasamsung.biz/tata-bx-tb.php?_t=1615176815](https://tatasamsung.biz/tata-bx-tb.php?_t=1615176815) which is pretending itself as an offer from TATA actually redirected us to the same type of Adidas campaign.

**In Depth Investigation:**

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited have looked into this matter to reach a conclusion that these websites are either legitimate or an online fraud.

Some key findings are --

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>oovip[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.203.12, 104.21.82.150</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:** D218547963-CNIC

**Registrar WHOIS Server:** whois.namesilo.com

**Registrar URL:** https://www.namesilo.com

**Updated Date:** 2021-02-04T15:16:38.0Z

**Creation Date:** 2021-01-21T03:23:27.0Z

**Registry Expiry Date:** 2022-01-21T23:59:59.0Z

**Registrar:** NameSilo, LLC

**Registrar IANA ID:** 1479

**Name Servers:** KURT.NS.CLOUDFLARE.COM

RUTH.NS.CLOUDFLARE.COM
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>phonesvip[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.49.154, 172.67.191.45</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: D223965693-CNIC

Registrar WHOIS Server: whois.namesilo.com

Registrar URL: https://www.namesilo.com

Updated Date: 2021-03-01T03:06:37.0Z

Creation Date: 2021-03-01T02:48:31.0Z

Registry Expiry Date: 2022-03-01T23:59:59.0Z

Registrar: NameSilo, LLC

Registrar IANA ID: 1479

Name Server: KAYLEIGH.NS.CLOUDFLARE.COM

           HARLAN.NS.CLOUDFLARE.COM
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>v-app[.]buzz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.132.36, 104.21.12.120</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: D42DED965BBD942A0BE8582D98AA07C98-NSR

Registrar WHOIS Server: whois.namesilo.com

Registrar URL: www.namesilo.com

Updated Date: 2021-02-24T06:35:18Z
Creation Date: 2021-02-19T06:35:13Z
Registry Expiry Date: 2022-02-19T06:35:13Z

Registrar: NameSilo, LLC
Registrar IANA ID: 1479

Name Server: hassio.ns.cloudflare.com
emely.ns.cloudflare.com
During the investigation we found another domain **adidastore[,]xyz** which is associated with the Adidas campaign.

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>adidastore[,]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.137.123, 104.21.81.15</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**: D224881483-CNIC

**Registrar WHOIS Server**: whois.namesilo.com

**Registrar URL**: https://www.namesilo.com

**Updated Date**: 2021-03-07T14:15:14.0Z

**Creation Date**: 2021-03-07T14:07:37.0Z

**Registry Expiry Date**: 2022-03-07T23:59:59.0Z

**Registrar**: NameSilo, LLC

**Registrar IANA ID**: 1479

**Name Server**: CARTER.NS.CLOUDFLARE.COM

**Name Server**: RACHEL.NS.CLOUDFLARE.COM
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>tatasamsung[.]biz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.28.236, 172.67.147.202</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**: D2E50DBA44F0F43318499765B48D3D507-NSR  

**Registrar WHOIS Server**: whois.namesilo.com  

**Registrar URL**: https://www.namesilo.com  

**Updated Date**: 2021-03-07T13:30:06Z  

**Creation Date**: 2021-03-07T13:17:45Z  

**Registry Expiry Date**: 2022-03-07T13:17:45Z  

**Registrar**: NameSilo, LLC  

**Registrar IANA ID**: 1479  

**Name Server**: roan.ns.cloudflare.com  

millie.ns.cloudflare.com
In source code analysis we found some information like --

- Title of the sites https://phonesvip[.]xyz/hw/ludo.php#XX and https://adidastore[.]xyz/adidas-s/#XX are ‘Amazon Women's Day Gift’ and ‘Adidas Women's Day gift’ respectively.

- 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. Everytime the website is visited, the section viz. time of the comments always remains the same.

During the investigation we found that some of the profile pictures linked in the comment section were used on the internet many times.
Users are insisted to share the campaign with WhatsApp friends and groups.

```javascript
function incrementValue1() {
    j = tiaoban = "hw/index.php?v=20210206";
    if (parseInt(getCookie('prog')) > 200) {
        window.open('whatsapp://send?text=');
    } else {
        window.open('whatsapp://send?text=' + j);
    }
    setTimeout(function () {
        
    }
}
```

We found some Chinese language written in the source code.

```javascript
// var url_share = items[share_num]['share_link'];
// var share_text = items[share_num]['share_desc'];
// var randomItem = share_text = "* " + url_share
// window.open('whatsapp://send?text=' + randomItem)
// window.open('whatsapp://send?text=' + j + '答对问题以获取情人节礼物。我参加了此问卷并赢得了手机，我的朋友也获得了奖品，未获得奖品：
window.open('whatsapp://send?text=' + j + ');
```

After translating in English we found --

"🎉❤️ Answer the questions to get Valentine’s Day gifts. I participated in this questionnaire and won a mobile phone. My friend also won prizes. To get prizes

This means the same theme was being used for Valentine’s Day campaigns.

Google tag manager id found G-TZT1MFLVY for the campaign.

```html
<script async src="https://www.googletagmanager.com/gtag/js?id=G-TZT1MFLVY"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());
gtag('config', 'G-TZT1MFLVY');
</script>
```

The campaign collects browser data and system data from the device.
During the investigation, we noticed users can win Huawei Mate 40 Pro 5G Full Netcom 8GB + 256GB (bright black) or Adidas ‘SUPERSTAR’ after completing the third attempt only.

Conclusive Summary:

- The campaign is pretended to be an offer from Amazon or Adidas but hosted on the third party domain instead of the official Amazon or Adidas website which makes it more suspicious.
- The domain names associated with the campaign have been registered in very recent time.
- During the investigation we have noticed multiple redirection 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.
- All the websites have different content but all of them follow the same type of mechanism and procedure to attract the users.
- The campaign collects browser and system information as well as the cookie data from the users.
- Getting into this type of a trap could lead the users to face whole system compromisation as well as massive financial loss.
- We recommend people to always keep away from such types of messages sent through social platforms. Always think before clicking on any links or downloading any attachments from unauthorised sources.

Issued by:

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