Research Report on:

“Answer the questions to receive Valentine’s Day gifts” scam
DISCLAIMER

This report is based on purely technical findings made by the research team during the investigation. It is not intended to malign or in any way target any country, actor or person through the findings. All the information provided in the report has been extracted during the investigation.
The Research Wing at CyberPeace Foundation has received some links via Whatsapp asking people to participate in a questionnaire to win Mobilephone, gift card etc. as a Valentine Day gift.

Case Study:

The Research wing at CyberPeace foundation along with the Research wing of Autobot Infosec Private Limited started an in depth investigation on the links to come to a conclusion that the campaign is either legitimate or an online fraud.

During the investigation the link https://www.pmvfym.cn/tiaoban.php?app=tata redirects us to https://www.thzmqhw.cn/index.php?app=shopee&sta=24#

On the landing page a Congratulations! appears with a paragraph which says about remaining time to take the gift followed by a section with some survey questions.
We have noticed, everytime the link is opened it redirects users to different domains having different contents.

As per our initial analysis it seems that the redirection to the different domains depend on the location or the region of the users.

→ https://www[.]thzmqhw[.]cn/index[.]php?app=shopee&sta=24#

As we mentioned above, on the landing page a Congratulations!! appears with a paragraph which says about remaining time to take the gift followed by a section having the survey questions.

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.
In the survey section some questions are being asked like *Are you Male or Female?, What is your Age? And Which is your Favourite device like Android or Apple?*. After completing the survey it says that *You have a chance to win Galaxy S21.*

After that the user is given three attempts to win the prize.
After completing the attempts it says **'Congratulations! You did it! You won the Galaxy S21!'**

Now 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 complete registration in order to get the prize.
After clicking on the green **Complete registration** button it redirects the user to a link

https://ddgonn.wintheprizes.net/c/f83bb5674dd1bf80?s1=95297&s2=1213159&s3=&s5=backuser&click_id=&ixpp=1&j1=1&j3=1

where another loyalty program with spin wheel can be seen.


As we mentioned earlier every time the link https://www.pmvfym.cn/tiaoban.php?app=tata is opened it redirects users to different domains with different contents, we got a new link https://www.aktmup.cn/index.php?app=walmart&sta=23 after the redirection.

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.
Like the first one, 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: a gift card worth $200. 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 complete registration in order to get the prize.

![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.](complete_registration.png)

After clicking on the green **Complete registration** button it redirects the user to a link **https://ddgonn.win-theprizes[.]net/c/f83bb5674dd1bf80?s1=95297&s2=1213159&j1=1&j3=1**

Also on this page we have noticed some type of Loyalty program having spin wheels as like the first link.

![LOYALTY PROGRAM
Friday, 12 February 2021
Congratulations!
Today you are lucky!
We select 7 users to give them the opportunity to win prizes from our sponsors. Turn the wheel to see which prize you will receive!](loyalty_program.png)
In Depth Investigation:

Some key findings can be mentioned as:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th><a href="http://www.pmvfym%5B.%5Dcn">www.pmvfym[.]cn</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.18.96, 172.67.181.141</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>

ROID: 20200406s10001s28304859-cn
Domain Status: ok

Registration Time: 2020-04-06 18:14:08
Expiration Time: 2021-04-06 18:14:08

Registrant: 唐源 (Tang Yuan)
Registrant Contact Email: 1340187681@qq.com

Sponsoring Registrar: 四川域趣网科技有限公司 (Sichuan Domain Fun Network Technology Co., Ltd.)

Name Server: bethany.ns.cloudflare.com
Name Server: fred.ns.cloudflare.com

DNSSEC: unsigned

**Chinese language detected.**
<table>
<thead>
<tr>
<th>Domain Name</th>
<th><a href="http://www.thzmqhw%5B.%5Dcn">www.thzmqhw[.]cn</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.50.181, 172.67.164.189</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>

ROID: 20200425s10001s28760829-cn  
Domain Status: ok  
Registration Time: 2020-04-25 10:22:49  
Registrant: 唐源 (Tang Yuan)  
Registrant Contact Email: 1340187681@qq.com  
Sponsoring Registrar: 四川域趣网科技有限公司 (Sichuan Domain Fun Network Technology Co., Ltd.)  
Name Server: evan.ns.cloudflare.com  
Name Server: tani.ns.cloudflare.com  
DNSSEC: unsigned  

**Chinese language detected.**
<table>
<thead>
<tr>
<th>Domain Name</th>
<th><a href="http://www.aktmup%5B.%5Dcn">www.aktmup[.]cn</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.64.175.22, 172.64.174.22</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>

ROID: 20200406s10001s28304719-cn
Domain Status: ok

Registration Time: 2020-04-06 18:12:38
Expiration Time: 2021-04-06 18:12:38

Registrant: 唐源 (Tang Yuan)
Registrant Contact Email: 1340187681@qq.com

Sponsoring Registrar: 四川域趣网®科技有限公司 (Sichuan Domain Fun Network Technology Co., Ltd.)

Name Server: bethany.ns.cloudflare.com
Name Server: fred.ns.cloudflare.com

DNSSEC: unsigned

**Chinese language detected.**
HTTP/1.1 200 OK

Date: Fri, 12 Feb 2021 12:09:33 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: __cfduid=db4f0daad172f30a944098d5f71af88601613131772; expires=Sun, 14-Mar-21 12:09:32 GMT; path=/; domain=.thzmqhw.cn; HttpOnly; SameSite=Lax
Vary: Accept-Encoding
Set-Cookie: shopee_user_visitor=visitor
CF-Cache-Status: DYNAMIC
cf-request-id: 0837be8a8a00002a573c887000000001
Report-To: [{"group":"cf-nel","endpoints": [{"url":"https://V/a.net.cloudflare.com/vreport/s=NiaQfKWcihoTPqaFfSLhL8ax4a%2B56NsQxw5PJ%2B5tf%2F%2FbEGU7uCZ9PjA2ITLJqhjDKyFqKEcEcpO9%2F%2BHkNh%2F53AnokEfM JHSXweA%3D%3D"}],"max_age":604800}]
NEL: [{"report_to":"cf-nel","max_age":604800}]
Server: cloudflare
CF-RAY: 6206338a79fa2a57-IAD
In source code analysis we found some information like:

- Title of the sites https://www.[]thzmqhw[.]cn/index[.]php?app=shopee&sta=24# and https://ww-w[.]aktmup[.]cn/index[.]php?app=walmart&sta=23 are "Happy Carnival 😁" and "1970th anniversary celebration" respectively.

- 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 v.z time of the comments always remains the same.

```
<div class="comment-content">
  <p class="name">Marvin Allen</p>
  <p>I like these promotions!</p>
</div>
```

```
<div class="comment-content">
  <p class="name">Casey Daniels</p>
  <p>I received my iPhone 12 Pro today. Thanks a lot!</p>
</div>
```

Piece of HTML code for fake Facebook comment section
Piece of CSS codes for fake Facebook comment section

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

- https://i.imgur.com/1H2Gelw.jpg
- https://i.imgur.com/AAKwzHS.jpg
- https://i.imgur.com/IhePd0v.jpg
- https://i.imgur.com/SMfVBNU.jpg
- https://i.imgur.com/T5yM1yR.jpg
- https://i.imgur.com/aM50FsF.jpg
- https://i.imgur.com/gg3teDe.jpg
- https://i.imgur.com/jxB4c6.jpg
- https://i.imgur.com/k5iYIls.jpg
- https://i.imgur.com/rWJaWux.jpg
- https://i.imgur.com/sQZsRZH.jpg
- https://i.imgur.com/wYUu4Np.jpg
From the piece of code written in javascript it is confirmed that users can only win the prize of $200 in the second chance.

```javascript
function startSpin() {
    var e = document.getElementById("spin"),
        n = document.getElementById("win"),
        t = document.getElementById("win2"),
        o = document.getElementById("win3"),
        s = document.getElementById("spinAround2"),
        m = document.getElementById("win5"),
        r = document.getElementById("win6");,
    e.className = e.className + " spinAround",
    n.style.display = "none",
    t.style.display = "block",
    s.style.display = "block",
    o.style.display = "none",
    m.style.display = "none",
    r.style.display = "none",
    setTimeout(function() {
        wxalert("You Won 1 Free Extra Spin!", "OK", 2, function()
        {
            spin2enabled = 10;
        });
    }, 6500);
}

function spin2() {
    if (spin2enabled) {
        var e = document.getElementById("spin"),
            n = document.getElementById("win"),
            t = document.getElementById("win2"),
            o = document.getElementById("win3"),
            s = document.getElementById("spinAround2"),
            m = document.getElementById("win5"),
            r = document.getElementById("win6");
        e.className = e.className + " spinAround2",
        n.style.display = "none",
        t.style.display = "none",
        o.style.display = "block",
        s.style.display = "block",
        m.style.display = "none",
        r.style.display = "block",
        setTimeout(function() {
            wxalert("Congratulations: 2", "Your prize: a gift card worth $200. Please:
            S(".hide-all") hide(), S(".show-all") show();
        });
    }
}
```

Piece of JS code to lure users to win prize

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

```javascript
function shareQBtn() {
    window.open(g_share_ad)
}

function shareBtn() {

    var share_num = get_Cookie('prog') == "" ? 0 : parseInt(get_Cookie('prog'))
    share_num++
    if (share_num > g_share_step) {
        share_num = g_share_step
    }
    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)

    setTimeout(function () {
        get_Cookie('prog') == "" ? value = 1 : value = parseInt(get_Cookie('prog'))
        shareStat(value)
        if (value > g_share_step) {
            shareStat(value)
        } else {
            value = 2 || value == 4 ? alert("Sharing failed! The same group or the same friend")
            if (value > 3 && g_banner_ad == false) {
                var qe = Math.round(Math.random() * 1000000)
                set_Cookie('banner_ad_share', "iframe src='https://uprinx.com/bnr_xload.php?section q_ban
```
• Google tag manager id found UA-186893005-15
  For both the link https://www.[.]thzmqhw[.]cn/index[.]php?app=shopee&sta=24#
  and https://www.[.]aktmup[.]cn/index[.]php?app=walmart&sta=23

  → https://www.googletagmanager.com/gtag/js?id=UA-186893005-15

• We found some encrypted code in the source code.

  Piece of Encrypted Code
Some of the other links found engaged with the same type of Campaign:

1. https://ddgonn[.]wintheprizes[.]net/c/f83bb5674dd1bf80?s1=95297&s2=1213326&j1=1&j3=1
2. https://www[.]mpgd3[.]cn/tiaoban[]php?app=tata
3. https://www[.]msc5ove[.]cn/tiaoban[]php?app=tata

Conclusive Summary:

- 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 layman users.

- The sites contain encrypted javascript code which could steal user’s personal data from their device using some malicious activities.

- Most of the domains found during the investigation have the .cn extension which indicates the country code of China.

- All the websites are having different content, but all of them follow the same type of mechanism and procedure to attract the users.

Issued By:

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