Research Report On:
Part-Time *Job Scam* On *WhatsApp*
Disclaimer

This report is based on purely technical findings made by the research team. It is not intended to malign or in any way target any country, actor or person through the findings. All findings made are with subsequent evidence provided in the report.
Research Report On: Part-Time Job Scam On WhatsApp

The Research Wing at CyberPeace Foundation has received some links via WhatsApp claiming one can earn 200 to 3000 Indian rupees by doing work from home only.

There is a part-time job, you can use your mobile phone to operate at home, you can earn 200-3000 rupees a day, 10-30 minutes a day, new users join to get you 50 rupees, waiting for you to join.

Reply 1 and long click the link to join us asap.

http://wame.wp-e.com/api/tg/wa/61VNfdR

http://wame.wp-e.com/api/tg/wa/61VNfdR

http://wame.wp-e.com/api/tg/wa/61VNfdR

Case Study

Links

http://wame.wp-e[.]com/api/tg/wa/QvROuQs

http://wame.wp-e[.]com/api/tg/wa/JZg6kJJ

http://wame.wp-e[.]com/api/tg/wa/8w36ceh

http://wame.wp-e[.]com/api/tg/wa/+91890240

http://wame.wp-e[.]com/api/tg/wa/91085176

http://wame.wp-e[.]com/api/tg/wa/61VNfdR

http://wame.wp-e[.]com/api/tg/wa/gkhe3ax
During the investigation whenever we surf to website normally using browser all Links are redirecting to URL https://wa.me/+91935496?text=hi

Chat on WhatsApp with +91 93549 6

CONTINUE TO CHAT

hi

Don’t have WhatsApp yet?
Download

Each link uses different number to send message

**Outgoing Links for all Links**

```
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=es
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=mk
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=et
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=tl
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=it
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=sk
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=pt_pt
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=kk
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=pl
https://api.whatsapp.com/send/?phone=%2B91817812\&text=hi\&app_absent=0\&lang=tr
```
Here, in all the links same outgoing links are used, just Numbers varies in all links after looking to all links you can observe that parameter "lang=" it shows that these links can be redirect to all languages other than English language to whatsapp inn other regions.

**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 the campaign is either legitimate or an online fraud.

**Analysis of Redirection**

We found info related to Cookies like Link is generating some JSESSIONID while surfing to URL as shown below the request and response.

Here, it is showing IP address also of Link where it is redirecting i.e. 47.75.111.165 and found some detail about that IP address. In all links same request is generated just the Numbers varies in request.
Associated IP Address Details

<table>
<thead>
<tr>
<th>Source</th>
<th>Whois.arin.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>47.75.111.165</td>
</tr>
<tr>
<td>Name</td>
<td>ALICLOUD-HK</td>
</tr>
<tr>
<td>Handle</td>
<td>NET-47-75-0-0-1</td>
</tr>
<tr>
<td>Registration Date</td>
<td>7/9/18</td>
</tr>
<tr>
<td>Range</td>
<td>47.75.0.0 – 47.75.255.255</td>
</tr>
<tr>
<td>Customer</td>
<td>ALICLOUD-HK</td>
</tr>
<tr>
<td>Customer Handle</td>
<td>C07018570</td>
</tr>
<tr>
<td>Address</td>
<td>26/F, Tower One, Times Square, 1 Matheson Street, causeway Bay, Hong Kong</td>
</tr>
<tr>
<td>City</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>Country</td>
<td>China</td>
</tr>
</tbody>
</table>

These IP address is of Alibaba Cloud, City Hong Kong and Country China as you see above.

Location (Approximate) (22.2909, 114.15)

More Details

<table>
<thead>
<tr>
<th>Net-Name</th>
<th>ALICLOUD-HK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Handle</td>
<td>NET-47-75-0-0-1</td>
</tr>
<tr>
<td>Parent</td>
<td>AL-3(NET-47-74-0-0-1)</td>
</tr>
<tr>
<td>Net Type</td>
<td>Reassigned</td>
</tr>
<tr>
<td>Origin AS</td>
<td>AS45102</td>
</tr>
<tr>
<td>Organisation</td>
<td>Alibaba.com LLC (AL-3)</td>
</tr>
<tr>
<td>Reg-Date</td>
<td>2018-07-09</td>
</tr>
<tr>
<td>Updated</td>
<td>2018-07-09</td>
</tr>
</tbody>
</table>

Origin AS number Details:

<table>
<thead>
<tr>
<th>AS45102</th>
<th>CN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>CN</td>
</tr>
<tr>
<td>Registration Date</td>
<td>2008-02-01</td>
</tr>
<tr>
<td>Registrar</td>
<td>Apnic</td>
</tr>
<tr>
<td>Owner</td>
<td>CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd., CN</td>
</tr>
</tbody>
</table>
These AS45102 is used by many other websites also

(a). phoinos.com

(b). Zoomerry.com

(c). Chinafree.online
(d). zoom-inn.com

zoom-inn.com
The domain is for sale!

If you are interested in this domain name, please contact the email above.

(e). suitianhose.com

Replica S.T.Dupont Lighter Zone

Replica S.T.Dupont Lighter offers an unmatched high quality collection that can simply be bought off the shelf without any second thoughts. Dupont artisans keep in mind all the minute details of the original product while creating the Replica lighter. The materials在线的 makes them all the more valuable and much preferred. Our collection of Replica S.T.Dupont Lighters are much affordable prices to meet the needs of our customers. We sell Replica S.T.Dupont Lighters which are almost identical in look and design when compared with the original S.T.Dupont Lighter. Making a replicate statement was made easy just to suit your budget and style.

A total of 52 units Replica S.T.Dupont Lighter online sales

- Replica S.T.Dupont Lighter (20)
- Replica S.T.Dupont Lighter (50)
- Replica S.T.Dupont Lighter (70)
- Replica S.T.Dupont Lighter (90)

USD 50.00
USD 60.00
USD 70.00
USD 80.00
USD 90.00
USD 100.00
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>wame.wp-e[.]com</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>47.75.111.165</td>
</tr>
<tr>
<td>ISP</td>
<td>Alibaba</td>
</tr>
<tr>
<td>ASN</td>
<td>45102</td>
</tr>
<tr>
<td>Country</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Registry Domain ID: 2557393669_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com

Updated Date: 2020-09-03T01:53:12Z
Creation Date: 2020-09-03T01:53:11Z
Registrar Registration Expiration Date: 2021-09-03T01:53:11Z

Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505

Registrant State/Province: Hong Kong
Registrant Country: CN (China)

Name Server: NS13.DOMAINCONTROL.COM
               NS14.DOMAINCONTROL.COM
DNSSEC: unsigned

Some similar links like these are also mentioned below

URLs hosted on the same domain

http://wame.wp-e.com/api/tg/wa/QvROuQs
http://wame.wp-e.com/api/tg/wa/81XGgbh
http://wame.wp-e.com/api/tg/wa/PHHP4yN
http://wame.wp-e.com/
http://wame.wp-e.com/api/tg/wa/8w36ceh
http://wame.wp-e.com/api/tg/wa/ceCncJq
http://wame.wp-e.com/api/tg/wa/F4xDOWT
http://wame.wp-e.com/api/tg/wa/1d0niOD

Certificate detail

HTTPS - 443
Certificate validation errors: RemoteCertificateNameMismatch
Signature algorithm: sha256RSA
Public key size: 2048 bits
Issuer: CN=Encryption Everywhere DV TLS CA - 01, OU=www.digicert.com,
        Subject: CN=vn.cliang.shop
Subject Alternative Name: DNS Name=vn.cliang.shop
Serial number: 00688846D5EB4056BC40D866B0B4CE5F
Not valid before: 2020-10-20 00:00:00Z
Not valid after: 2021-10-20 23:59:59Z
SHA1 fingerprint: D1A13CAC6BDC96E157CB48CC916DF5583A9AE36

HTTP/1.1 403 Forbidden
Server: nginx/1.16.1
Date: Tue, 05 Jan 2021 11:35:44 GMT
Content-Type: text/html
Content-Length: 153
Connection: close
DNS Records

DNS records

DNS query for 165.111.75.47.in-addr.arpa returned an error from the server: NameError

<table>
<thead>
<tr>
<th>name</th>
<th>class</th>
<th>type</th>
<th>data</th>
<th>time to live</th>
</tr>
</thead>
<tbody>
<tr>
<td>wame.wp-e.com</td>
<td>IN</td>
<td>A</td>
<td>47.75.111.165</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>wp-e.com</td>
<td>IN</td>
<td>A</td>
<td>23.227.38.32</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>wp-e.com</td>
<td>IN</td>
<td>NS</td>
<td>ns13.domaincontrol.com</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>wp-e.com</td>
<td>IN</td>
<td>NS</td>
<td>ns14.domaincontrol.com</td>
<td>3600s (01:00:00)</td>
</tr>
<tr>
<td>wp-e.com</td>
<td>IN</td>
<td>SOA</td>
<td>server: ns13.domaincontrol.com&lt;br&gt;email: <a href="mailto:dns@jomax.net">dns@jomax.net</a>&lt;br&gt;serial: 2020123101&lt;br&gt;refresh: 86400&lt;br&gt;retry: 7200&lt;br&gt;expire: 604800&lt;br&gt;minimum ttl: 600</td>
<td>3600s (01:00:00)</td>
</tr>
</tbody>
</table>

Link Details for http://wame.wp-e.com/api/tg/wa/61VNfdR

In all links same redirection and outgoing sources are generated but in last link i.e. above mentioned link (given in whatsapp chat photo in mail) some different things were observed.

We found some different URL while scanning for this link as shown below:

http://wa.zbcweb.xyz/?num=+91767829 &text=hi

After that we have started analysing these Link and found results:

HTTP Response

Final URL
http://wa.zbcweb.xyz/?num=+91767829 &text=hi

Serving IP Address
149.129.179.69

Status Code
200
### Domain Name

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>wa.zbcweb[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>149.129.179.69</td>
</tr>
<tr>
<td>ISP</td>
<td>Alibaba</td>
</tr>
<tr>
<td>ASN</td>
<td>45102</td>
</tr>
<tr>
<td>Country</td>
<td>Singapore</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

**Registry Domain ID:** D209851988-CNIC  
**Registrar WHOIS Server:** whois.godaddy.com  
**Registrar URL:** https://www.godaddy.com/  
**Updated Date:** 2020-12-17T17:29:01.0Z  
**Creation Date:** 2020-11-20T09:13:58.0Z  
**Registry Expiry Date:** 2021-11-20T23:59:59.0Z  
**Registrar:** Go Daddy, LLC  
**Registrar IANA ID:** 146

**Registrant State/Province:** Hong Kong  
**Registrant Country:** CN (China)

**Name Server:** NS75.DOMAINCONTROL.COM  
**Name Server:** NS76.DOMAINCONTROL.COM  
**DNSSEC:** unsigned

Here we found one new IP Address and after investigation of IP address (149.129.179.69) we found that IP Address belongs to one of the China's E-Commerce website which is hosted on Alibaba Cloud.

### Numbers Associated with all Links

Doing online investigation on the numbers we found some details—

1. +91-817812 (Location: - Delhi)

<table>
<thead>
<tr>
<th>Phone Number</th>
<th>+91-817812</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>India</td>
</tr>
<tr>
<td>Carrier</td>
<td>Reliance Telecom Pvt Ltd</td>
</tr>
<tr>
<td>Is Wireless</td>
<td>Yes</td>
</tr>
</tbody>
</table>
2. +91-879979
   (Location: - Delhi)
   | Phone Number       | +91-879979       |
   | Country            | India            |
   | Carrier            | Reliance Telecom Pvt Ltd |
   | Is Wireless        | Yes              |

3. +91-885197
   (Location: - Delhi)
   | Phone Number       | +91-885197       |
   | Country            | India            |
   | Carrier            | Reliance Telecom Pvt Ltd |
   | Is Wireless        | Yes              |

4. +91-890240
   (Location: - Kolkata)
   | Phone Number       | +91-767829       |
   | Country            | India            |
   | Carrier            | Vodafone ESSAR South Ltd |
   | Is Wireless        | Yes              |

5. +91-767829
   (Location: - Delhi)
   | Phone Number       | +91-767829       |
   | Country            | India            |
   | Carrier            | Reliance Telecom Pvt Ltd |
   | Is Wireless        | Yes              |

6. +91-951527
   | Phone Number       | +91-951527       |
   | Country            | India            |
   | Carrier            | Bharti Airtel Ltd |
   | Is Wireless        | Yes              |
URL Manipulation

Link: - http://wame.wp-e.com/api/tg/wa/code

In all links after removing directory ‘code’ when we enter the website then some error message arises in webpage

This message is written in Chinese language, after converting it we found that it is Internal Server Error 500

Here, there is one link given to redirect to homepage as shown in above figure in red box. This Link redirects the page to homepage of this domain.
These shows that server is using CentOS and when we surf website with only /api/ part in link then it shows some error in Chinese language.

404
找不到网页！
对不起，您正在寻找的页面不存在。尝试检查URL的错误，然后按浏览器上的刷新按钮或者尝试在我们的应用程序中找到其他内容。主页

After translation we found that

404
I can't find the page!
Sorry, the page you are looking for does not exist. Try checking for errors in the URL, then press the refresh button on your browser or try to find something else in our application. Home.
Conclusions:

- The domain names found during the investigation seem somehow registered from China.
- By url manipulation we found that the error codes are shown in Chinese language.

Issued by:

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