RESEARCH REPORT ON
FAKE COVID SUBSIDY SCHEME
OF INR 50,000 - 1,00,000

CyberPeace
Foundation
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 of CyberPeace Foundation received some links via WhatsApp which claim people can earn INR 50000 as COVID-19 subsidy.

**Link:**

http://amt8.7s.7eospo.com/jp/1621078212.html  
http://6fr2.2.7ausafo6americans.com/jp/1621404149.html

**Case Study:**

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.

On visiting both of the links users were redirected to the link http://stephenharker[.]com/#XX.

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

On the landing page a congratulations message appears with the offer details which promises to give a subsidiary of 50000 INR to 100000 INR in the name of the Coronavirus Foundation.
Upon scrolling further down, it asks the user to answer a few questions like mentioned below.

**Question 1 of 4:** are you male or female?
- male
- female

**Question 2 of 4:** How old are you?
- 18-29
- 30-39
- 40-49
- 50+

**Question 3 of 4:** What do you think about the new corona virus?
- Does not matter
- Its so bad!
- It really affected my life

**Question 4 of 4:** Have you and your family or friends been infected with the new corona virus?
- Themselves infected
- The Family has been infected
- Friends has been infected
- Not infected

Once the user finishes the survey a congratulatory message is displayed.

"Congratulations, you have passed the official Foundation audit!"

Congratulations, you have passed the official Foundation audit!
You have the opportunity to receive cash subsidies for the coronavirus disease outbreak in India!
Click to claim

On clicking the ‘Click to claim’ button the users are again displayed a congratulatory message and it prompts users to share the campaign over WhatsApp.

congratulations!

You are eligible for the subsidy and receive INR50,000 rupee from the Coronavirus Foundation. The final step to receive.
***rules***
1. You have to tell 5 groups or 20 friends to let more people know about our rescue plan and help them.
2. After the distribution is successful, we will release it to your bank account.

Click to claim
When the user clicks on the "Click to claim" it prompts the user to a WhatsApp button and asks the user to share some personal information like Name, Phone Number etc.

Name:

phone:

Submit

On the final attention it shows users a message

"Information submitted successfully".

Information submitted successfully
Congratulations on your completion. Due to the large number of participants, our staff will contact you after verification within 3-5 days!

WhatsApp
In Depth Analysis:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>amtb8.77esport[.]com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>47.241.9.153</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>

**Domain Name:** 77esport.com  
**Registry Domain ID:** 9974594418_DOMAIN_COM-VRSN  
**Registrar WHOIS Server:** whois.west.cn  
**Registrar URL:** www.west.cn

**Registrar:** Chengdu west dimension digital technology Co., LTD  
**Registrar IANA ID:** 1556

**Updated Date:** 2019-06-03T20:37:16.0Z  
**Creation Date:** 2019-06-03T20:37:16.0Z  
**Registrar Registration Expiration Date:** 2021-06-03T20:37:16.0Z

**Registrant State/Province:** zhe jiang  
**Registrant Country:** CN (China)

**Name Server:** jm1.dns.com  
**Name Server:** jm2.dns.com
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>6fr2e.usaforamericans[.]com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>47.241.191.160</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>

**Domain Name:** usaforamericans.com  
**Registry Domain ID:** 2551607520_DOMAIN_COM-VRSN  
**Registrar WHOIS Server:** whois.55hl.com  
**Registrar URL:** http://www.55hl.com

**Registrar:** JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD  
**Registrar IANA ID:** 1469  
**Registrar Abuse Contact Email:** abuse@55hl.com  
**Registrar Abuse Contact Phone:** +86.2586883426 ext 1009

**Updated Date:** 2020-08-08T01:38:00Z  
**Creation Date:** 2020-08-08T01:37:36Z  
**Registrar Registration Expiration Date:** 2021-08-08T01:37:36Z

**Registrant State/Province:** guangdong  
**Registrant Country:** CN (China)  
**Name Server:** jm1.dns.com  
jm2.dns.com
During the phase of analysis especially focused on the background behaviour of the site we noticed a simultaneous connection was being established to a domain listentome.oss-ap-southeast-1.aliyuncs.com.
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>listentome.oss-ap-southeast-1[.]aliyuncs.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>47.74.196.87</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>

**Domain Name:** ALIYUNCS.COM  
**Registry Domain ID:** 1710447560_DOMAIN_COM-VRSN  
**Registrar WHOIS Server:** grs-whois.hichina.com  
**Registrar URL:** http://www.net.cn  

**Registrar:** Alibaba Cloud Computing (Beijing) Co., Ltd.  
**Registrar IANA ID:** 420  
**Registrar Abuse Contact Email:** DomainAbuse@service.aliyun.com  
**Registrar Abuse Contact Phone:** +86.95187  

**Updated Date:** 2021-02-16T21:50:10Z  
**Creation Date:** 2012-04-01T07:23:40Z  
**Registry Expiry Date:** 2023-04-01T07:23:40Z  

**Registrant State/Province:** zhe jiang  
**Registrant Country:** CN (China)  

**Name Server:**  
- NS3.ALIYUN.COM  
- NS4.ALIYUN.COM  
- NS5.ALIYUN.COM
Conclusive Summary:

- The campaign is pretended to be an offer from “Coronavirus Foundation”, if the foundation really exists the campaign should have been hosted on the official website of the respective foundation instead of any third-party domain which makes it more suspicious.

- During the investigation we have noticed multiple redirections between the links.

- The prizes are kept really attractive to lure the laymen.

- All the domain names associated with the campaign have the registrant country as China.

- During the phase of analysis especially focused on the background behaviour of the site we noticed a simultaneous connection was being established to a domain listentome.oss-ap-southeast-1.[.]aliyuncs.com. Which again belongs to China.

CyberPeace Advisory:

- CyberPeace Foundation recommends that people avoid opening such messages sent via social platforms. One must always think before clicking on such links, or downloading any attachments from unauthorized sources.

- Falling for this trap could lead to whole system compromisation (Access to microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications etc.) as well as financial loss for the users. One must always think before clicking on such links, or downloading any attachments from unauthorized sources.

- Do not share confidential details like login credentials, banking information with such a type of scam.

- Never share or forward fake messages containing links with any social platform without proper verification.

Issued by:

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