Research Report on

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A FREE 30 GB DATA SCAM

IN NAME OF VARIOUS INTERNET PROVIDER COMPANY
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 and information might be changed after generating the reports.
The Research Wing of CyberPeace Foundation received a link via Whatsapp related to the 30 GB Free Data Azadi Offer.

3. VI, https://cli.re/VI-30GB

Summary

**WARNING SIGNS**

- The campaign is pretended to be an offer from various internet provider companies but is hosted on the third-party domain instead of the official internet provider website which makes it more suspicious.
- The domain names associated with the campaign have been registered in very recent times.
- Multiple redirections have been noticed between the links.
- No reputed site would ask its users to share the campaign on WhatsApp.
- The prize is kept really attractive to lure the laymen.
- Grammatical mistakes have been noticed.

**CYBERPEACE ADVISORY**

- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms.
- Falling into this trap could lead to whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as the financial loss for the users.
- Do not share confidential details like login credentials, and banking information with such a type of scam.
- Never share or forward fake messages containing links to any social platform without proper verification.
- There is a need for International Cyber Cooperation between countries to bust the criminal gangs running fraud campaigns affecting individuals and organisations to make Cyberspace resilient and peaceful.
Case Study

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited has looked into this matter to reach a conclusion that the website is either legitimate or online fraud.

On Visiting the link users were redirected to

https://fill2.us/Claim-Now#1660625698151

**Where XX represents a unique 13 digits number, for example 1660625698151.**

On the landing page, there is an attractive image of Tricolor and a message that says 15th August Offer 30GB Free Data.

At the bottom of this page, there is a section that seems like a social-media comment section.
The user has to enter the phone number and internet service provider company name.

After selecting the above given network

“After Verification, You have been qualified to get free Recharge. How to proceed!

- How to activate your free 30 GB offer?
- Share it with 5 groups or 15 friends on WhatsApp (Click on SHARE ICON below)
- You will be redirected automatically to our free recharge page after the GREEN verification bar is filled
- You will receive a confirmation by SMS in 15 minutes”

After Clicking the SHARE button users are given to install a Google Play Store app.

Link:

IN DEPTH INVESTIGATION:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th><a href="https://fill2%5B.%5Dus/Claim-Now">https://fill2[.]us/Claim-Now</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ OK ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.220.142</td>
</tr>
<tr>
<td>ISP</td>
<td>CloudFlare.Inc</td>
</tr>
<tr>
<td>ASN</td>
<td>13335</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>

Domain Name: https://fill2[.]us/Claim-Now

Registrant State/Province: Torson David
Registrant Country: Pakistan (pk)
Registrant Org: Torson

Updated Date: 6/7/2022
Creation Date: 29/6/2022
Registry Expiry Date: 29/6/2023

Name Server: SAGE.NS.CLOUDFLARE.COM
Name Server: STEVIE.NS.CLOUDFLARE.COM
**SOURCE CODE ANALYSIS:**

- The title of the page is "30 GB Azaadi Offer".

- We found three Google tag manager ids (G-YSZ8S8C2VB) in the source code.

- 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.
Users are insisted on sharing the campaign with WhatsApp friends and groups.

We found a get request is going to this domain(pro.ip-api.com), this api is used to get the data about users with the city, region, zip, country, continent, timezone, latitude.
CONCLUSIVE SUMMARY:

The campaign is pretended to be an offer from various internet service providers but hosted on the third-party domain instead of the official website which makes it more suspicious.

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

We have investigated the URLs in a secured sandbox environment where the WhatsApp application was not installed. If any user opens the link from a device like a smartphone where the 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.

The domain names associated with the campaign have been registered in very recent times.

Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front-end domain names used in this gift scam campaign.
CyberPeace Advisory:

CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.

If at all, the user gets into this trap, it could lead to a whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as financial losses.

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

Do not share or forward fake messages containing links without proper Verification.

There is a need for International Cyber Cooperation between countries to bust the cybercriminal gangs running the fraud campaigns affecting individuals and organizations, to make Cyberspace resilient and peaceful.

Issued by:

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