RESEARCH REPORT ON

“AMAZON VALENTINE’S DAY GIFTS” SCAM

CyberPeace Foundation
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 and information might be changed after generating the reports.
The Research Wing of CyberPeace Foundation received a link via Whatsapp related to a free gift campaign pretending to be an offer from Amazon which asks users to participate in a short quiz in order to get a chance to win 15,000 free gifts.

**Link:**

https://tinyurl2[.]ru/m045130551/

**Case Study:**

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

On Visiting the link users were redirected to https://tinyurl2[.]ru/m045130551/#XX.

**Where XX represents a unique 13 digits number, for example 1633075913900.**

On the landing page a Welcome message appears with an attractive photo of Amazon products and asks users to participate in a short quiz in order to get Valentine’s day gifts.
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.

The quiz starts with some basic questions like Do you know Amazon?, How old are you?, What you think about Amazon?, Would you recommend us to your friends? etc

Once the user answers the questions a “congratulatory message” is displayed.
“Congratulations!
Your answer has been saved successfully!

You have a chance to win gifts.
You must select the correct box with your prize inside.
You have 3 attempts. Good luck!”

After clicking the OK button, users are given three attempts to win the prizes with multiple gift boxes.

After completing all the attempts, it says that the user has won "Apple iPhone 11 128GB".

“Congratulations! You did it! You have won the prize Apple iPhone 11 128GB”
Clicking on the ‘OK’ button, it instructs users to share the campaign on WhatsApp.

![WhatsApp Share Button](image)

Strangely enough the user has to keep clicking the WhatsApp button until the progress bar completes.

After clicking on the green ‘share’ button multiple times it shows a section where again a congratulations appears.

![Congratulations Page](image)

Very good! The last step:

1. You must complete the form to get your gift by clicking on "FINISH".

(Remember: This step is very important)

After completing the above instructions, wait for the administrator's review, which will be completed within 24 hours.

![Finish Button](image)

After clicking on the green “Complete Registration” button, it redirects the user to multiple advertisements webpages and it varies each time the user clicks on the button.
In Depth Investigation:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>tinyurl2[.]ru</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>172.67.186.238, 104.21.2.85</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>

Whois Data:

domain: TINYURL2.RU
state: REGISTERED, DELEGATED, VERIFIED
person: Private Person
registrar: R01-RU
admin-contact: https://partner.r01.ru/contact_admin.khtml
created: 2022-01-30T12:16:48Z
paid-till: 2023-01-30T12:16:48Z
free-date: 2023-03-02
source: TCI
HTTP Response Header:

Link: https://tinyurl2[]ru/m045130551/

<table>
<thead>
<tr>
<th>HTTP/1.1 200 OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date: Fri, 11 Feb 2022 07:08:22 GMT</td>
</tr>
<tr>
<td>Content-Type: text/html</td>
</tr>
<tr>
<td>Transfer-Encoding: chunked</td>
</tr>
<tr>
<td>Connection: close</td>
</tr>
<tr>
<td>Last-Modified: Fri, 11 Feb 2022 02:24:05 GMT</td>
</tr>
<tr>
<td>Cache-Control: max-age=14400</td>
</tr>
<tr>
<td>CF-Cache-Status: MISS</td>
</tr>
<tr>
<td>Expect-CT: max-age=604800, report-uri=&quot;<a href="https://report-url.cloudflare.com/cdn-cgi/expect-ct">https://report-url.cloudflare.com/cdn-cgi/expect-ct</a>&quot;</td>
</tr>
</tbody>
</table>
| Report-To: 
  {
    "endpoints": [{
      "url": "https://\V/a.nel.cloudflare.com\report\v3?i=Z1HC5tKer000Eeg7Gjw3ccKY37FbEOtdfR%2FX7wD1dbTJnhingpk60gn1daoFW
vXduliiA1dHYv55wf00c2XDBFdlv1yDyIyTjmqvb9
9nVwWm5v9k3Ef0b3KIMZPlg%3D%3D"}],
    "group": "cf-nel",
    "max_age": 604800
  }
| NEL: 
  {
    "success_fraction": 0,
    "report_to": "cf-nel",
    "max_age": 604800
  }
| Server: cloudflare |
| CF-RAY: 6d8bedbc8c181a3-IAD         |
| alt-svc: 
  h3="":443",
  ma=86400,
  h3-29="":443",
  ma=86400 |
In source code analysis we found some information like --

- The title of the site is **Amazon Valentine’s Day Gifts**

- 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.
With the purpose of pushing the notification and tracking the user, OneSignal SDK has been used.

```html
<script src="https://cdn.onesignal.com/sdk/OneSignalSDK.js"></script>
```

In background analysis we found a site `https://settrogens[.]com` was being connected which may trigger the injection of other malware or unwanted programs.

**URL:** `https://settrogens[.]com/link?z=4314551&var=exit&ymid={CLICK_ID}`

```javascript
for (t = 0; t < 10; t++) history.pushState({}, "", ")
onpopstate = function(t) {
  t.state & location.replace("https://settrogens.com/link?z=4314551&var=exit&ymid={CLICK_ID}"
  //var myUrl = "https://tinyurl2.ru/?w&Math.random().toString().slice(2,11) + ";
  //t.state & location.replace(myUrl)
}
```

**Request**

```
GET /link?z=4314551&var=pushPlt&ymid={CLICK_ID} HTTP/1.1
Host: settrogens.com
Sec-Ch-Ua: "Not A; Brand", "Chrome"; v="88", "Chromium"; v="88", "Google Chrome"; v="88"
Sec-Ch-Ua-Platform: "Android"
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Pragma: no-cache
Cache-Control: no-transform, no-store, no-cache, must-revalidate, max-age=0
Accept-Encoding: gzip, deflate
Accept-Language: en-US, en;q=0.9
Connection: close
```

**Response**

```
HTTP/2 200 OK
Server: nginx
Date: Fri, 11 Feb 2022 01:08:07 GMT
Content-Type: text/html; charset=utf-8
Content-Security-Policy: frame-origin https://settrogens.com
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding
Access-Control-Max-Age: 86400
Pragma: no-cache
Cache-Control: no-transform, no-store, no-cache, must-revalidate, max-age=0
Expires: Tue, 11 Jan 1994 10:00:00 GMT
Timing-Allow-Origin: *
You have answered all 4 questions

Your IP address is valid for this promotion

Gifts are available and in stock!

Congratulations! You did it! You have won the prize: Samsung Galaxy S22 Ultra.

*** THE RULES ***

1. You must inform 5 groups or 20 friends about our promotion.
2. Enter your address and complete the registration.

OK.

1. Share with 5 groups / 20 friends on WHATSAPP. (Tap the "WhatsApp" icon below)
2. Tap "Next" to receive the prize.

Very good! The last step: After completing the above instructions, wait for the administrator's review, which will be completed within 24 hours.
After decoding the script, it was found that the code contains all the details about what type of data to be fetched from the users.
The campaign collects browser and system information from the device.

```javascript
if ($(".p_var-browser").length >= 1) {
    var c = getBrowser();
    
    $(".p_var-browser").text(c);
}

if ($(".p_var-browser").length >= 1) {
    var e = getPlatform();
    
    $(".p_var-so").text(e);
}
```
Conclusive Summary:

- The campaign is pretended to be an offer from Amazon but hosted on the third party domain instead of the official website of Amazon 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 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.

- The domain used in the campaign has been registered recently.

- During the investigation we noticed the link redirects the user to a 404 error page if the user opens the link in the desktop computer. However if the link gets opened on a mobile device the campaign works fine. It means cybercriminals have targeted mainly mobile internet users through this campaign.

- Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front end domain name used in the campaign.

CyberPeace Advisory:

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

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

- Do not share confidential details like login credentials, 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 the Cyberspace resilient and peaceful.

Issued by:

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