RESEARCH REPORT ON

“CADBURY VALENTINE’S DAY CHOCOLATE GIVEAWAY” SCAM
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://tinyurl[.]su/u515905391/

**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://tinyurl[.]su/u515905391/#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 Cadbury chocolate 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 Cadbury? How old are you? What do you think about Cadbury? Would you recommend us to your friends?**

Once the user answers the questions a “congratulatory message” is displayed.
“Congratulations! your answers have been successfully saved.

This is your chance.

You must select the correct box with the gift 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 “Cadbury Dairy Valentine Heart Shaped Gift Box.”

“Congratulations!

You did it! You have won the prize Cadbury Dairy Valentine Heart Shaped Gift Box.”
Clicking on the ‘OK’ button, it instructs users to share the campaign on WhatsApp.

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

After clicking on the green ‘WhatsApp’ button multiple times it shows a section where instruction has been given in order to get the prize.

On clicking the green **FINISH** button, it redirects the user to multiple advertisement web pages 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</th>
<th><a href="https://tinyurl%5B.%5Dsu">https://tinyurl[.]su</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 OK</td>
</tr>
<tr>
<td>IP Address</td>
<td>111.90.145.248</td>
</tr>
<tr>
<td>ISP</td>
<td>Dosarrest Internet Security LTD</td>
</tr>
<tr>
<td>ASN</td>
<td>45839</td>
</tr>
<tr>
<td>Country</td>
<td>Malaysia</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

Domain Name: https://tinyurl[.]su

Registrar URL: https://r01.ru
Registrar: R01-SU

Registrar IANA ID:
Updated Date: 2010-07-30
Creation Date: 2021-12-09T17:54:53.000Z

Registry Expiry Date: 2022-12-09T17:54:53.000Z

Name Server: aspen.ns.cloudflare.com
brodie.ns.cloudflare.com
HTTP Response Header:

Link: https://tinyurl[]su/u515905391/

HTTP/1.1 200 OK

Server: nginx

Date: Tue, 15 Feb 2022 09:56:25 GMT

Content-Type: text/html

Content-Length: 96903

Last-Modified: Thu, 10 Feb 2022 12:21:49 GMT

Connection: close

ETag: "6205035d-17a87"

Accept-Ranges: bytes
In source code analysis we found some information like --

- The title of the site is **Cadbury Valentine's Day Chocolate Giveaway**

- 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.

<script src="https://cdn.onesignal.com/sdks/OneSignalSDK.js"></script>

- In background analysis we found a site [https://settrogens.com](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)](https://settrogens.com/link?z=4314551&var=exit&ymid=(CLICK_ID))

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

**Request**

```
GET /link?z=4314551&var=pushFaymid=(CLICK_ID) HTTP/1.1
Host: settrogens.com
Sec-Ch-Ua: " Not;A,Br,Brand";v="99", "Chromium";v="86", "Google Chrome";v="86"
Sec-Ch-Ua-Mobile: ?1
Sec-Ch-Ua-Platform: "Android"
Upgrade-Insecure-Requests: 1
Save-Data: on
User-Agent: Mozilla/5.0 (Linux; Android 7.0; Custom AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.4664.104 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
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 05:09:07 GMT
Content-Type: text/html; charset=utf-8
X-Trace-Id: 290e61494a724a75e6d01743e996a
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: *
Set-Cookie: 0AID=a055df800e440d053a27ae9ccc5b008; expires=Sat, 11 Feb 2022 05:09:07 GMT
```
Welcome to Cadbury Valentine's Day Giveaway!

Complete the short quiz and win an exclusive gift.

133 gifts left.

<p class="result" id="result1">
You have answered all 4 questions
</p>

<p class="result" id="result2">
Your IP address is valid for this promotion
</p>

<p class="result" id="result3">
Gifts are available and in stock!
</p>

<h2>Congratulations, your answers have been successfully saved.</h2>

This is your chance.

You must select the correct box with the gift inside.

You have 3 tries - good luck!

(src=https://i.imgur.com/L.ZC44.png)

Congratulations
You did it! You have won the prize
Cadbury Dairy Valentines Heart Shaped Gift Box.

*** THE RULES ***

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

1. Share with 5 groups / 20 friends on WHATSAPP. (tap the "WhatsApp" icon below)
2. Tap "Next" to receive the prize.
Some encoded script was found in the source code.

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-so").text(e);
} 
```
Conclusive Summary:

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