RESEARCH REPORT ON

“AMUL 75TH ANNIVERSARY”

SCAM
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 Amul which asks users to participate in a survey in order to get a chance to win Rs. 6000.

**Link:**

http://knowtaste[.]top/3624cQQAXVhfkJyXmi8Nw5YBE-F0DR4pU1IsFwE6KAaocMSIYfjYrEid1Pgs?awh1633859923660

**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 the link

https://preferabletask[.]xyz/t0htSRvk/Amul-wa/?_t=1633930907cpo#XX

**Where XX represents a unique 13 digits number, for example 1633930916000**

On the landing page a Congratulations message appears with an attractive photo of Amul Logo and asks users to participate in a quick survey in order to get a “2000 Euro”.
Also at the bottom of this page a section comes up which seems to be a comment section where many users have commented about how the offer is beneficial.

The survey starts with some basic questions like Do you know Amul? How old are you? What do you think of Amul? Are you male or female? etc

Question 1 of 4: Do you know Amul?
- Yes
- No

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

Question 3 of 4: How do you think of Amul?
- Very good
- Unbelievable
- OK
- Not so good

Question 4 of 4: Are you male or female?
- Male
- Female

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 prize.

After completing all the attempts it says that the user has won “2000 Euro”.

“Congratulations! You did it! You won 2000 Euro”
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 an instruction has been given to complete registration in order to get the prize.

![Registration screen](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</th>
<th>knowtaste[.]top</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 OK [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.16.40</td>
</tr>
<tr>
<td>ISP</td>
<td>Cloudflare, Inc.</td>
</tr>
<tr>
<td>ASN</td>
<td>AS15169</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>

Domain Name: knowtaste[.]top
Registry Domain ID: D20210924G10001G_69313950-top
Registrar WHOIS Server: whois.aliyun.com
Registrar URL: http://www.alibabacloud.com
Registrar: Alibaba.com Singapore E-Commerce Private Limited
Registrar IANA ID: 3775

Updated Date: 2021-09-24T09:32:57Z
Creation Date: 2021-09-24T06:58:11Z
Registry Expiry Date: 2022-09-24T06:58:11Z

Registrant Organization: huangxiao song
Registrant State/Province: jiang su
Registrant Country: CN (china)

Name Server: brit.ns.cloudflare.com
            quentin.ns.cloudflare.com
<table>
<thead>
<tr>
<th>Domain</th>
<th>preferabletask[.]xyz</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 OK [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>104.21.87.220</td>
</tr>
<tr>
<td>ISP</td>
<td>Cloudflare, Inc.</td>
</tr>
<tr>
<td>ASN</td>
<td>AS13335</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>

Domain Name: PREFERABLETASK[.]XYZ  
Registry Domain ID: D234602784-CNIC  
Registrar WHOIS Server: whois.namesilo.com  
Registrar URL: https://www.namesilo.com  
Registrar: NameSilo, LLC  
Registrar IANA ID: 1479  

Updated Date: 2021-05-27T13:56:12.0Z  
Creation Date: 2021-05-07T07:43:51.0Z  
Registry Expiry Date: 2022-05-07T23:59:59.0Z  

Registrant State/Province: AZ  
Registrant Country: US  

Name Server: IGNACIO.NS.CLOUDFLARE.COM  
AUTUMN.NS.CLOUDFLARE.COM
**Important**

During the analysis we found, in the background a javascript code called `hm.js` was being executed from the host `hm.baidu.com` which is a subdomain of Baidu and is used for Baidu Analytics, also known as **Baidu Tongji**.

**Note:** “Baidu is a Chinese multinational technology company specialising in Internet-related services, products and artificial intelligence, headquartered in Beijing’s Haidian district, China.”
https://en.wikipedia.org/wiki/Baidu

Query URL: 
- https://hm.baidu.com/js?a0e297c5bd68aa91c692ad78a7cc92c9
- https://hm.baidu.com/js?362571d334dfe4bbda42380c64db58ac
- https://hm.baidu.com/js?bbb3e86814c9ceef66d180a6c15fa17d

```
(function() {
    var hm = document.createElement("script");
    hm.src = "https://hm.baidu.com/hm.js?a0e297c5bd68aa91c692ad78a7cc92c9";
    var s = document.getElementsByTagName("script")[0];
    s.parentNode.insertBefore(hm, s);
})();
var _hmt = _hmt || [];
(function() {
    var hm = document.createElement("script");
    hm.src = "https://hm.baidu.com/hm.js?362571d334dfe4bbda42380c64db58ac";
    var s = document.getElementsByTagName("script")[0];
    s.parentNode.insertBefore(hm, s);
})();
var _hmt = _hmt || [];
(function() {
    var hm = document.createElement("script");
    hm.async = true;
    hm.src = "https://hm.baidu.com/hm.js?bbb3e86814c9ceef66d180a6c15fa17d";
    var ts = document.getElementsByTagName("script")[1];
    ts.parentNode.insertBefore(hm, ts);
```

<!DOCTYPE html>
<html>
<head><link rel="stylesheet" type="text/css" href="style.css" /></head>
<body>
</body>
</html>
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>hm.baidu[.]com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>103.235.46.191</td>
</tr>
<tr>
<td>ISP</td>
<td>Beijing Baidu, Netcom Science and Technology Co.</td>
</tr>
<tr>
<td>ASN</td>
<td>55967</td>
</tr>
<tr>
<td>Location</td>
<td>Hong Kong</td>
</tr>
<tr>
<td>Continent</td>
<td>Asia</td>
</tr>
</tbody>
</table>

**Domain Name**: baidu[.]com
**Registry Domain ID**: 11181110_DOMAIN_COM-VRSN
**Registrar WHOIS Server**: whois.markmonitor.com
**Registrar URL**: http://markmonitor.com
**Registrar**: MarkMonitor Inc.
**Registrar IANA ID**: 292

**Updated Date**: 2020-12-09T04:04:41Z
**Creation Date**: 1999-10-11T11:05:17Z
**Registrar Registration Expiration Date**: 2026-10-11T11:05:17Z

**Registrant Organization**: Beijing Baidu Netcom Science Technology Co., Ltd.
**Registrant State/Province**: Beijing
**Registrant Country**: CN (China)
Conclusive Summary:

- The campaign is pretended to be an offer from Amul but hosted on the third party domain instead of the official website of Amul 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 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 campaign collects browser and system information from the users.

- Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front end domain names used in this Amul 75th Anniversary campaign. But during the phases of investigation, we have identified a domain name that was requested in the background and has been traced as belonging to China.

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.