Catching the Facebook Scammer

Mantas Sasnauskas
About Me

Senior Information Security Researcher @CyberNews

Interests: Threat Hunting, Cybercrime, Data Leaks, Hardware Hacking, Astrophotography

My GitHub: https://github.com/lexcor
What happened?

Investigation into a malicious Facebook Messenger message uncovered a large-scale phishing operation on Facebook which led me to potentially identify the threat actor behind the phishing campaign and his intentions.
“Is that you” Phishing Scam

- “Is that you” is a phishing scam circulating on Facebook in various forms since at least 2017. It begins with a Facebook message sent by one of your friends. The “friend” claims to have found a video or image with you featured in it.
- The message masquerades as a video that, when clicked, leads you through a chain of websites infected with malicious scripts.
- These scripts determine your location, the device you are using, and your operating system. They then lead you to a malicious Facebook phishing page in order to harvest your credentials, and, depending on your device, infect it with adware or other malware and use the traffic for malvertising.
The Scale

THE MOST AFFECTED USERS BY COUNTRY

Germany
376,701 users

Percentage of Users: 77.06%  < 2%

United Kingdom
17,708 users

Percentage of Users: 73.28%  2 - 10%  < 2%
The Scale Now

<table>
<thead>
<tr>
<th>Country</th>
<th>Visitors</th>
<th>Percentage of Visitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Japan</td>
<td>295,671</td>
<td>43.23%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>287,164</td>
<td>41.99%</td>
</tr>
<tr>
<td>United States</td>
<td>12,436</td>
<td>1.82%</td>
</tr>
</tbody>
</table>
How?

- The campaign is initiated by sending the potential victim a message from one of their Facebook contacts. The message contains what appears to be a video link with a suggestive text that asks the victim ‘Is that you?’

- It seems that the message employs Facebook’s Open Graph protocol to manipulate the fake video preview to include the recipient’s name.
Phishing Page

- The malicious script that redirects victim to the phishing page is hidden in what appears to be a compromised legitimate website.
- http://108xxxxxxx.rsc.cdn77.org/Uploaded/Content/26d0ba85d866423db3d591c9835d72ef/saliendopadentro.xml
- The file has a small script that triggers a redirect to a short URL, which then leads the victim to a malicious phishing page. Using a legitimate website to host malicious redirect scripts makes the phishing attack more effective as it can be used to bypass Facebook’s blacklists.
The Tracking Code

- Discovery of a legitimate third-party service-tracking code implanted in the phishing page.
- After obtaining the identifier, we were able to access the threat actor’s dashboard to determine the scale of the campaign.
Some Stats

THE MOST AFFECTED USERS BY BROWSER

<table>
<thead>
<tr>
<th>Browser</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>12,277</td>
</tr>
<tr>
<td>Safari iPhone</td>
<td>11,206</td>
</tr>
<tr>
<td>Opera</td>
<td>39 users</td>
</tr>
<tr>
<td>Firefox</td>
<td>24 users</td>
</tr>
</tbody>
</table>

THE MOST AFFECTED USERS BY OPERATING SYSTEM

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>12,172</td>
</tr>
<tr>
<td>iOS</td>
<td>11,255</td>
</tr>
<tr>
<td>Windows</td>
<td>131 users</td>
</tr>
<tr>
<td>Mac</td>
<td>61 users</td>
</tr>
</tbody>
</table>
The Threat Actor

As I investigated the phishing page, I learned that it includes HTML content with Open Graph metadata and obfuscated images with Base64 encoding.
To my surprise, I found that the malicious script was signed by the author. Translated from Spanish, the author’s signature means:

```
1   //Desarrollado por
2   //BenderCrack.com
3
4   function sh(){
5       var h = document.getElementById("u_0_3");
6       var s = document.getElementById("u_0_4");
7       var p = document.getElementById("m_login_password");
```
I was able to identify and correlate other, potentially malicious activities that we traced to the same threat actor. The Facebook phishing campaign is named Tamo Trabajando, which means “we’re working.”
During continued investigation into the threat actors campaign, I also managed to correlate the following domains used for different phishing or scam campaigns.

- http://blacksar.xyz
- http://blacksar.in
- Http://blacksar.co
- Http://berafle.xyz
- Http://blacksar.date
- Http://blacksar.me
- Http://blacksar-dns.me
- http://bendercrack.com
The domain mentioned in the signature no longer exists. However, upon further investigation, I discovered a Facebook page that could be connected to the creator of the malicious script:
Motives
Malvertising and generating malicious traffic

http://tdrco2.com
AdsLeading - Let's grow together!!!
Top Awards for Top Affiliates. Check more details on AdsLeading Perks or register for free on our platform. 1. / 3. We create great opportunities for you!

```
1 <script>
2   try {
3       window.top.location.href = "https://tdrco2.com/";
4   } catch(e) {
5       // statements
6       window.location.href = "https://tdrco2.com/";
7   }
8 </script>
```

BenderCrack PRO
When you leave the password they enter the account, they send spam to friends when friends enter the link has advertising more or less 150 dollars for every thousand visits from the United States for example 😊
Motives

Malvertising and generating malicious traffic
One of the malicious Blacksar domains was registered from the Dominican Republic, which strongly suggests that the threat actor is from a Spanish-speaking country or even the Dominican Republic itself.

One interesting campaign and tracking code was LA PARITA, which tracked a particular personal Facebook profile and its visitors. That person seemed to be based in the Dominican Republic.
Thank you