OWASP

Open Web Application Security Project

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

OWASP
Open Web Application Security Project

What happened?

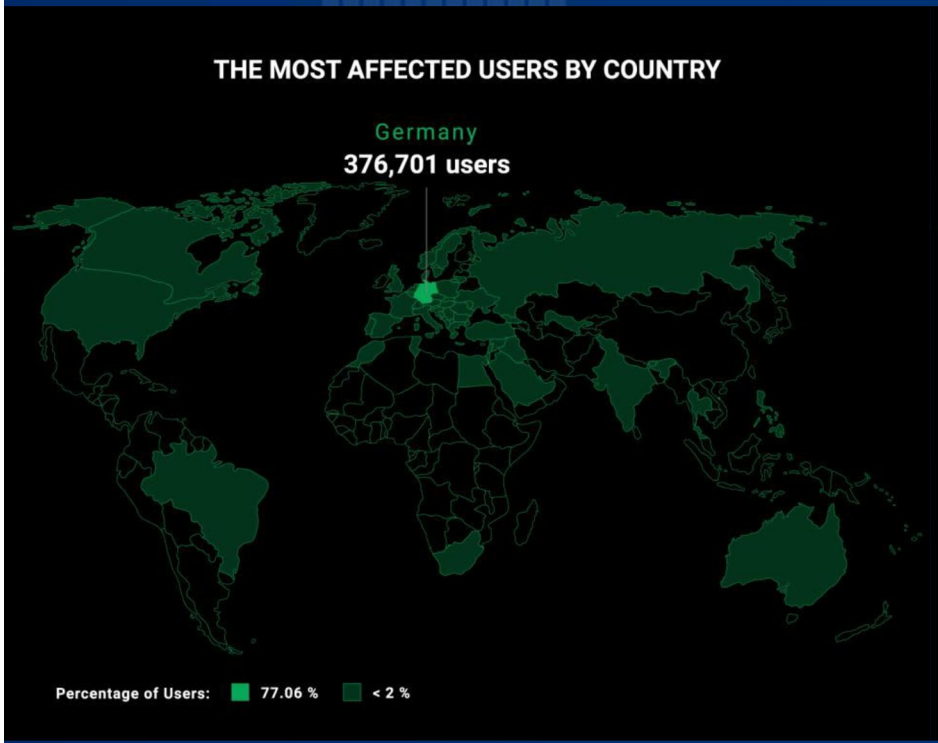
Investigation into a malicious Facebook Messenger message uncovered a large-scale phishing operation on Facebook which led me to potentially identify the threat actor behind the phishing campaign and his intentions.

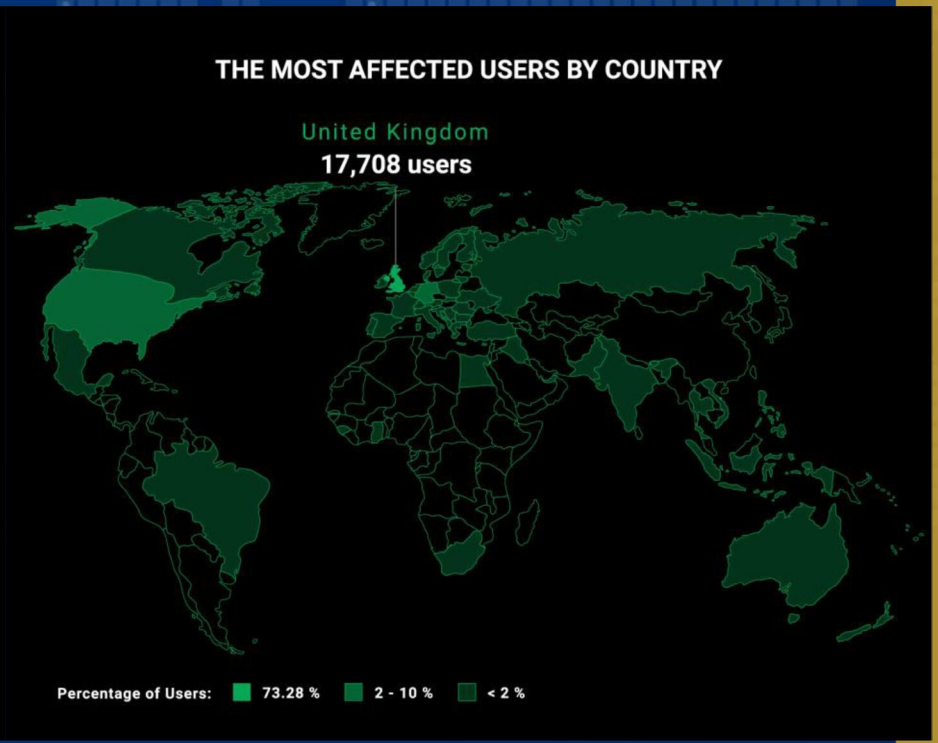
OWASP
Open Web Application Security Project

“Is that you” Phishing Scam

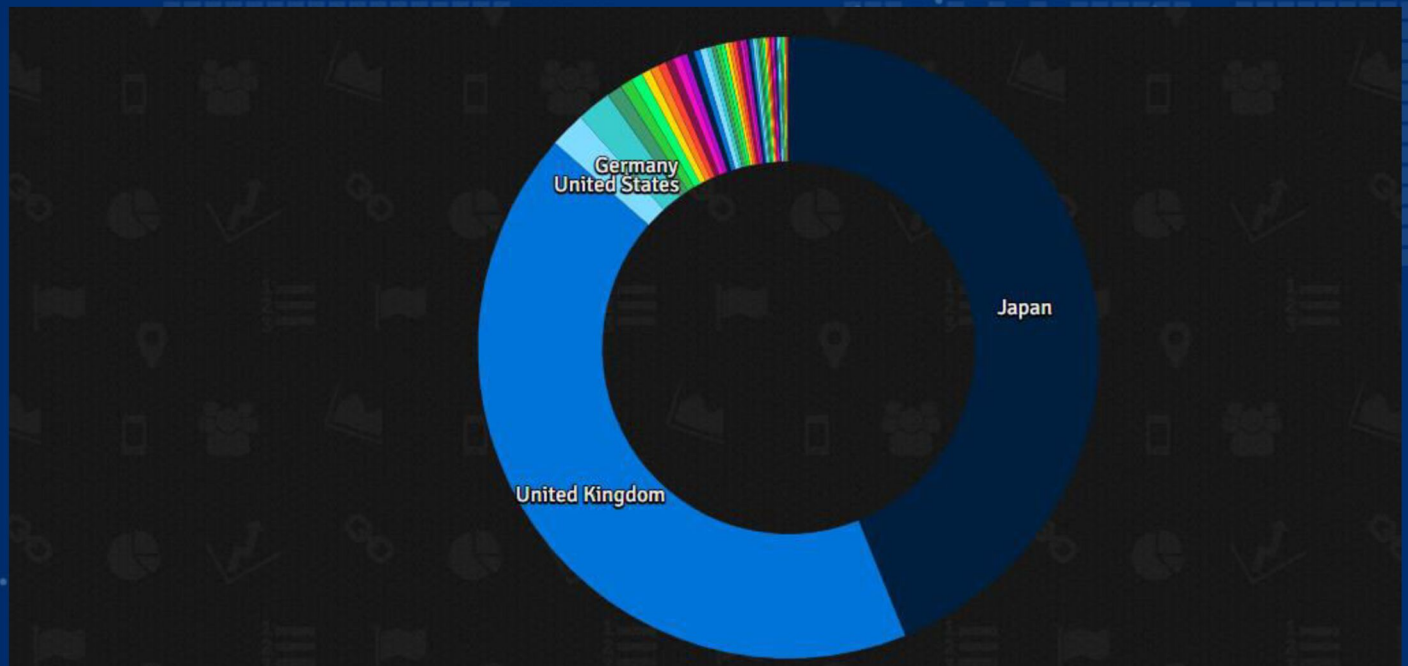
- “Is that you” is a phishing scam circulating on Facebook in various forms since at least 2017. It begins with a Facebook message sent by one of your friends. The “friend” claims to have found a video or image with you featured in it.
- The message masquerades as a video that, when clicked, leads you 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 %


THE MOST AFFECTED USERS BY COUNTRY
United Kingdom
17,708 users
Percentage of Users:
73.28 %
2 - 10 %
< 2 %

The Scale Now



Country	Visitors	Percentage of Visitors
Japan	295,671	43.23%
United Kingdom	287,164	41.99%
United States	12,436	1.82%

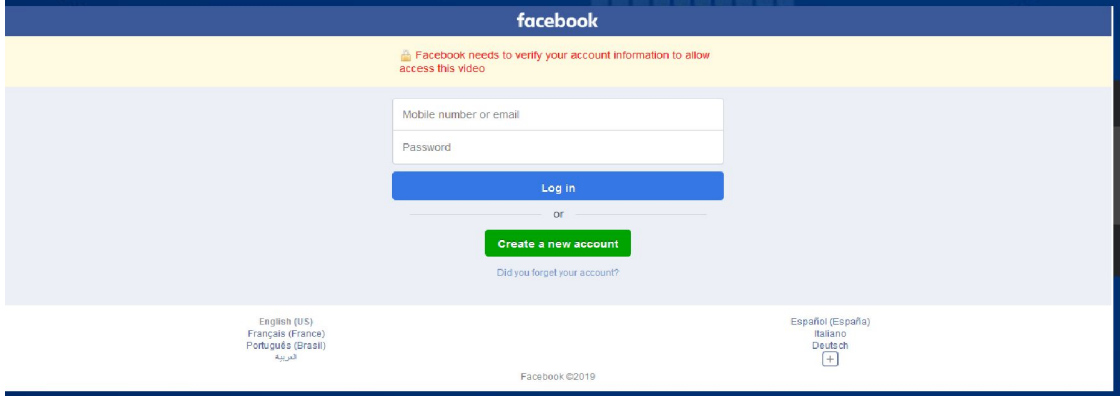
How?

- 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.




```
<script xmlns="http://www.w3.org/1999/xhtml">
  <![CDATA[
  window.location.href = 'http://wal.ee/
  ]]> == $0
</script>
```

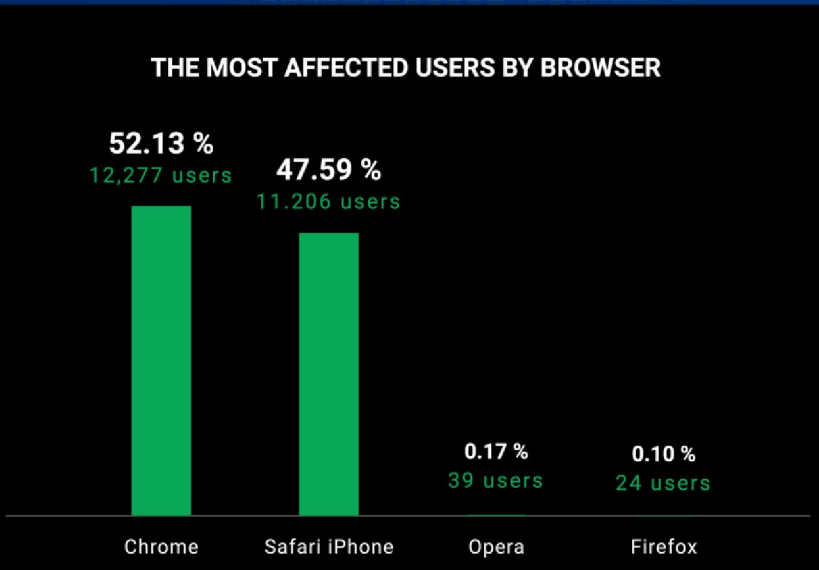
OWASP
Open Web Application Security Project

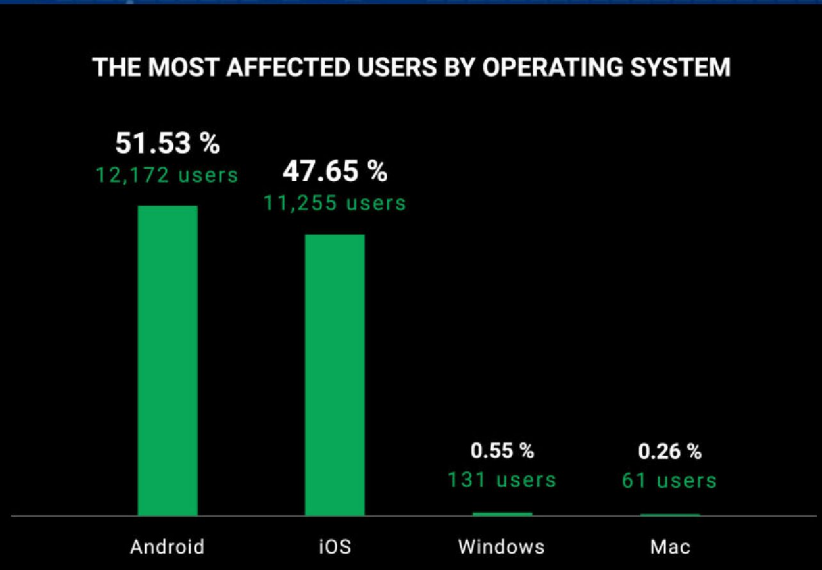
The Tracking Code

```
▶ <style>…</style>
▶ <div id="viewport" data-kaios-focus-transparent="1" style="min-height: 667px;">…</div>
  <img src="//whos.amung.us/pingjs/[redacted]" style="display:none" alt>
▶ <script>…</script>
▶ <script>…</script>
```

- 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
52.13 %
12,277 users
47.59 %
11.206 users
0.17 %
39 users
0.10 %
24 users
Chrome
Safari iPhone
Opera
Firefox


THE MOST AFFECTED USERS BY OPERATING SYSTEM
51.53 %
12,172 users
47.65 %
11,255 users
0.55 %
131 users
0.26 %
61 users
Android
iOS
Windows
Mac

The Threat Actor

OWASP
Open Web Application Security Project

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:

Developed by BenderCrack.com

```
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");
```

The Threat Actor

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.”

The Threat Actor

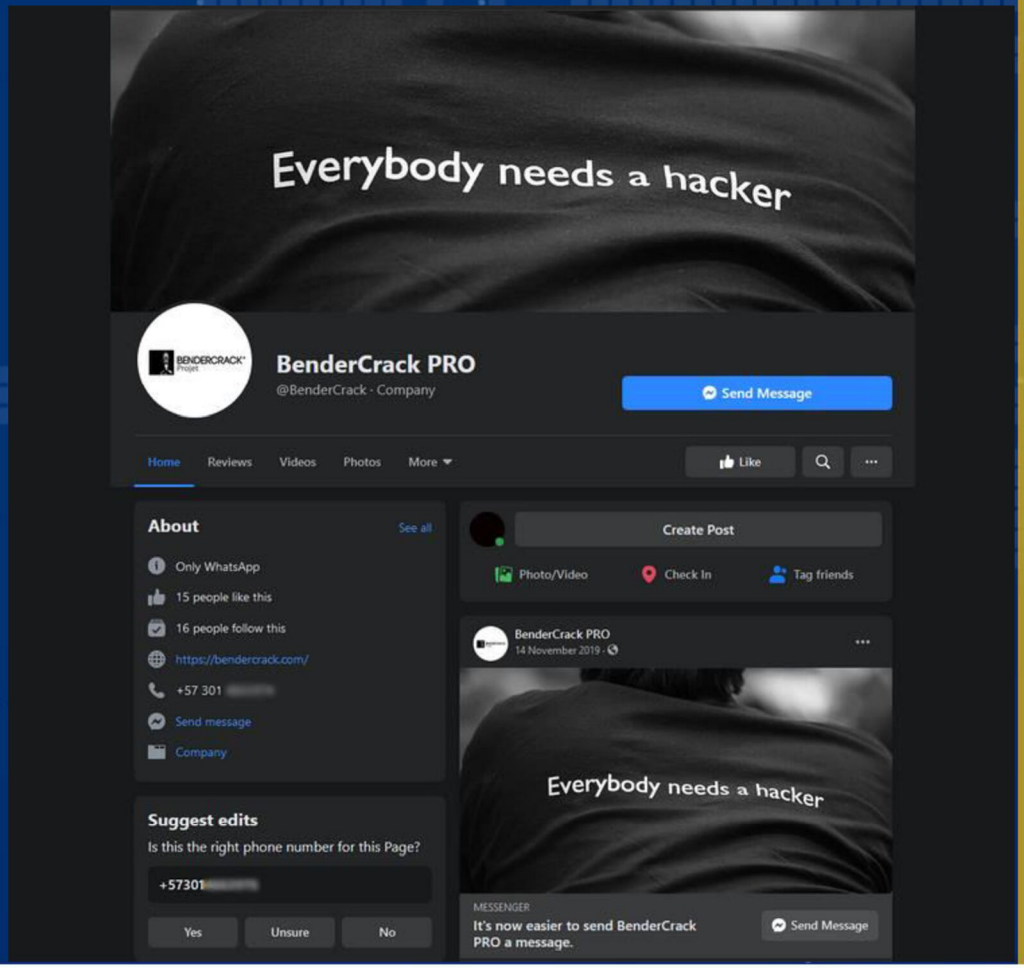
OWASP
Open Web Application Security Project

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**

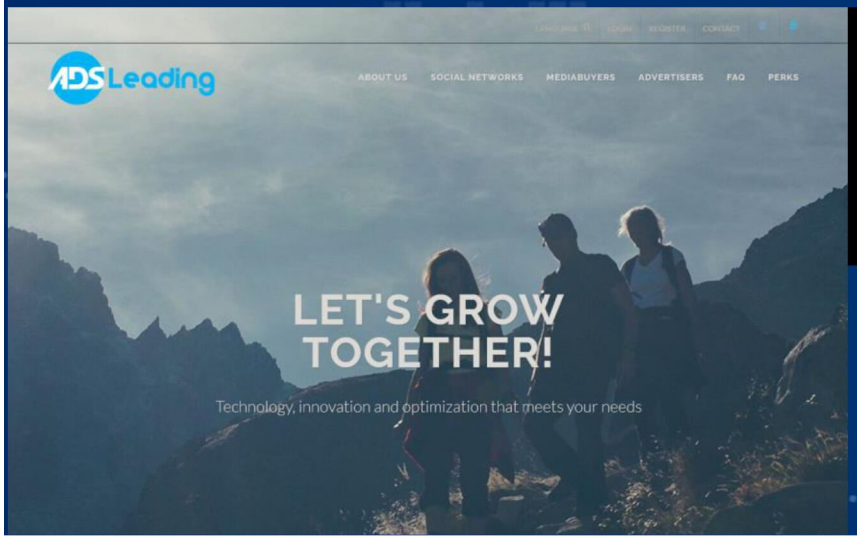
Threat Actor

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




```
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>
```

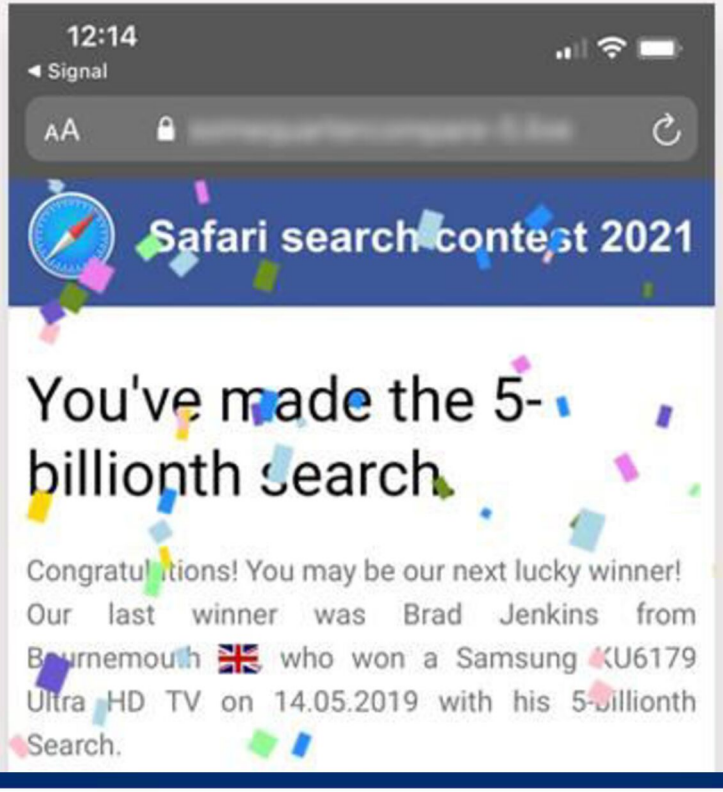
http://tdrco2.com

AdsLeading - Let's grow together!!!

Top Awards for Top Affiliates. check more details on AdsLeading Perks or register for free our platform. 1. /. 3. We create great opportunities for you!

Motives

Malvertising and generating malicious traffic



Dominican Republic

- 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.

Creation Date	2020-05-01T22:20:07 | 2020-05-01T22:20:07Z
DNSSEC	unsigned
Domain Name	BLACKSAR.DATE | blacksar.date
Domain Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited | client UpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server	dns10.blacksar-dns.me | dns11.blacksar-dns.me
Registrant City	1f8f4166599d23ee | 3432650ec337c945
Registrant Country	CA | DO

OWASP

Open Web Application Security Project

Thank you