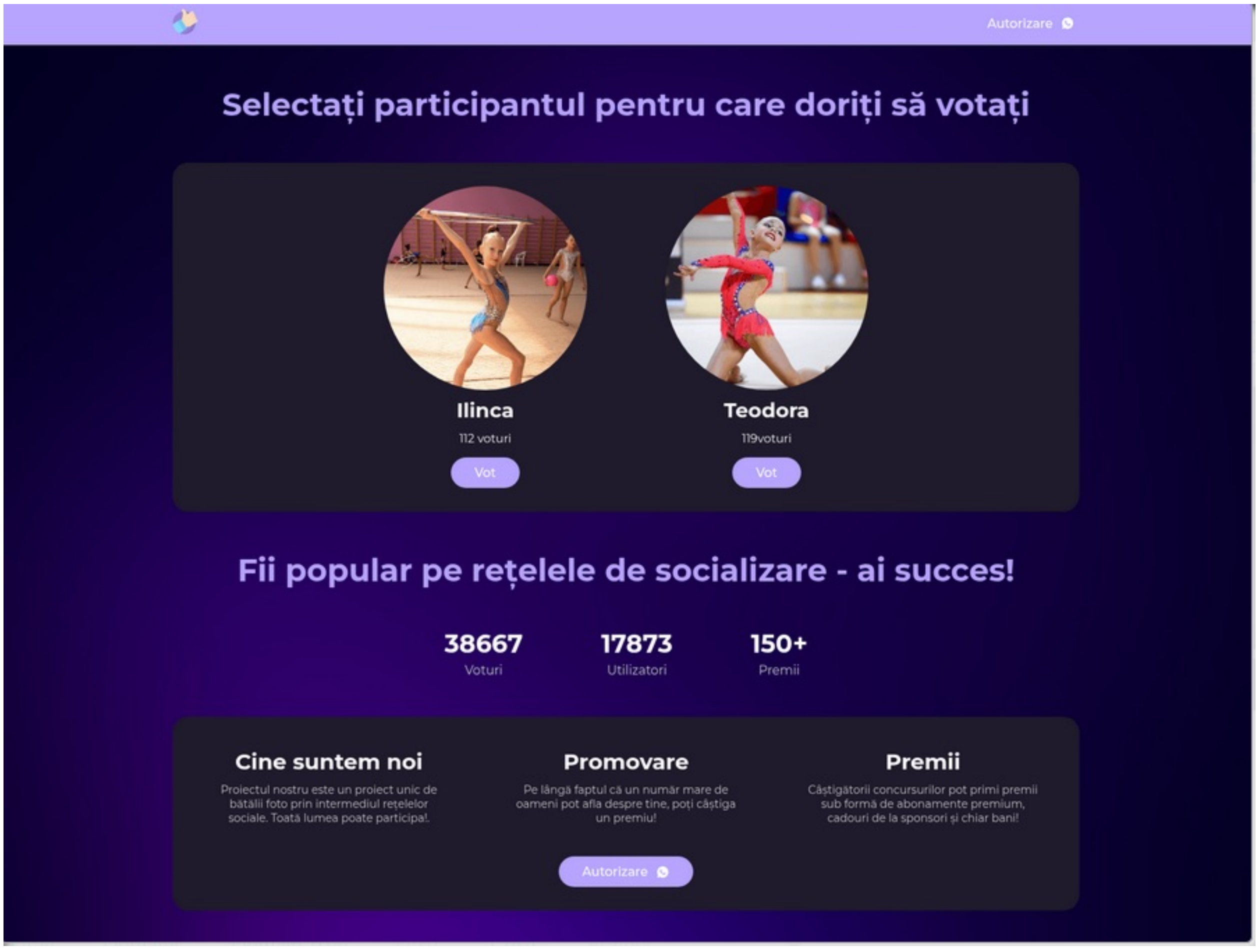
Russian campaign targeting Romanian WhatsApp numbers

cybergeeks.tech/russian-campaign-targeting-romanian-whatsapp-numbers/

We've identified a campaign that advises people to vote for a contest so they can win "prizes". The only "prize" is that they'll lose access to their WhatsApp account. Multiple hints indicate that the campaign originates from Russia. This article written in Romanian presents general details about this method.

Users receive a WhatsApp message from friends or family that were previously compromised in the campaign. The message is in Romanian and encourages the recipient to vote in a contest. An example of the suspicious URL is https[:]//concursro[.]com/home/vote4:



Selectați participantul pentru care doriți să votați

Fii popular pe rețelele de socializare - ai succes!

Cine suntem noi

Proiectul nostru este un proiect unic de bătălii foto prin intermediul rețelelor sociale. Toată lumea poate participa!.

Promovare

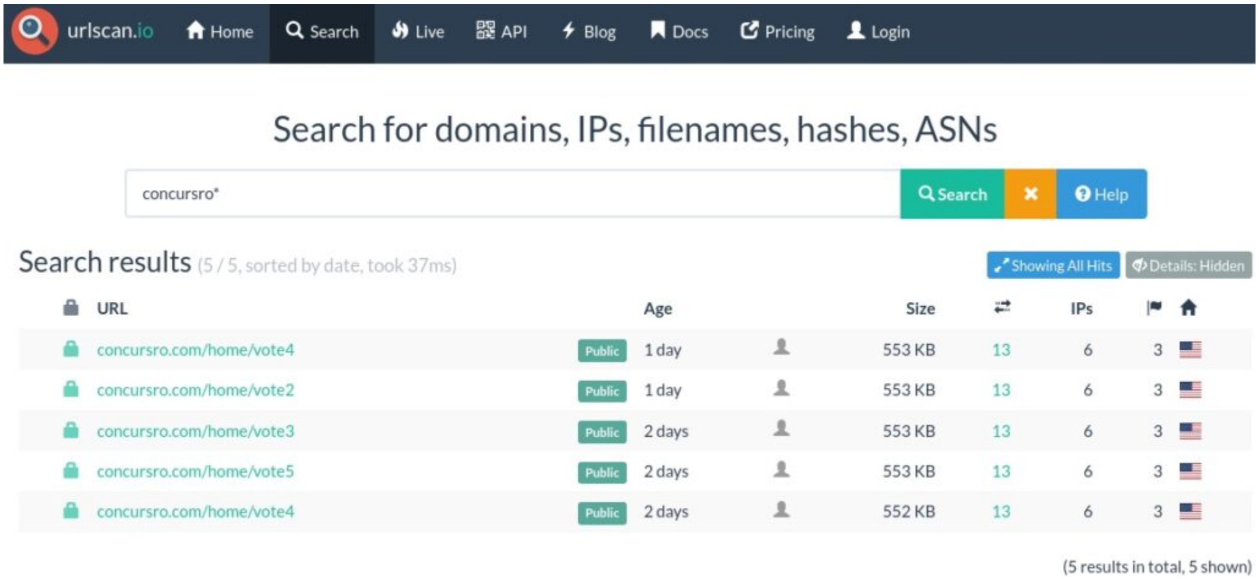
Pe lângă faptul că un număr mare de oameni pot afla despre tine, poți câștiga un premiu!

Premii

Câștigătorii concursurilor pot primi premii sub formă de abonamente premium, cadouri de la sponsori și chiar bani!

Figure 1

We've used Urlscan.io to identify other domains from the same campaign. As we can see in Figure 2, multiple URLs were sent:



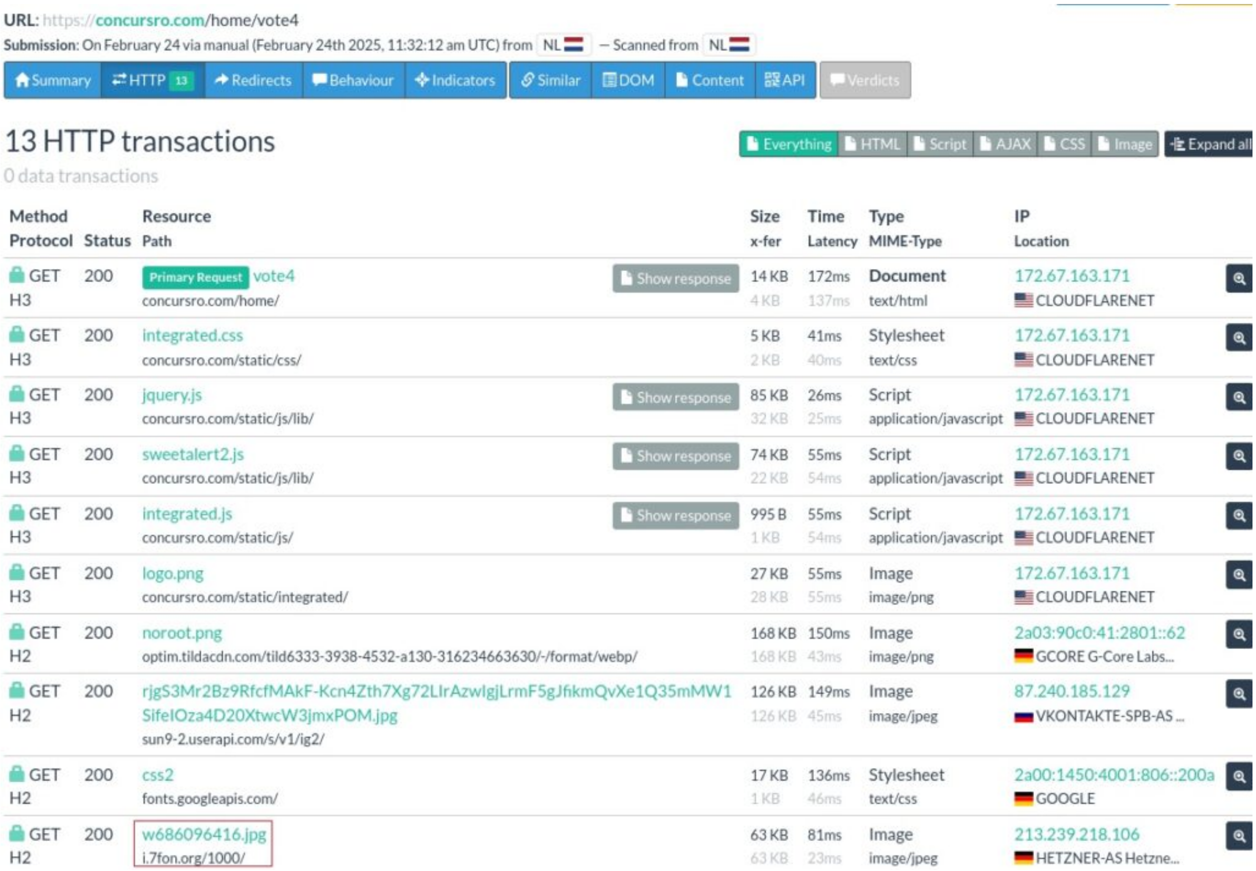
Search results (5 / 5, sorted by date, took 37ms)

URL		Age	Size	⇄	IPs		
concursro.com/home/vote4	Public	1 day	553 KB	13	6	3	🇺🇸
concursro.com/home/vote2	Public	1 day	553 KB	13	6	3	🇺🇸
concursro.com/home/vote3	Public	2 days	553 KB	13	6	3	🇺🇸
concursro.com/home/vote5	Public	2 days	553 KB	13	6	3	🇺🇸
concursro.com/home/vote4	Public	2 days	552 KB	13	6	3	🇺🇸

(5 results in total, 5 shown)

Figure 2

We’ve observed a GET request for an image called “w686096416.jpg” and another one for an image from the Russian social network VKontakte:



URL: https://concursro.com/home/vote4
Submission: On February 24 via manual (February 24th 2025, 11:32:12 am UTC) from NL 🇳🇱 — Scanned from NL 🇳🇱

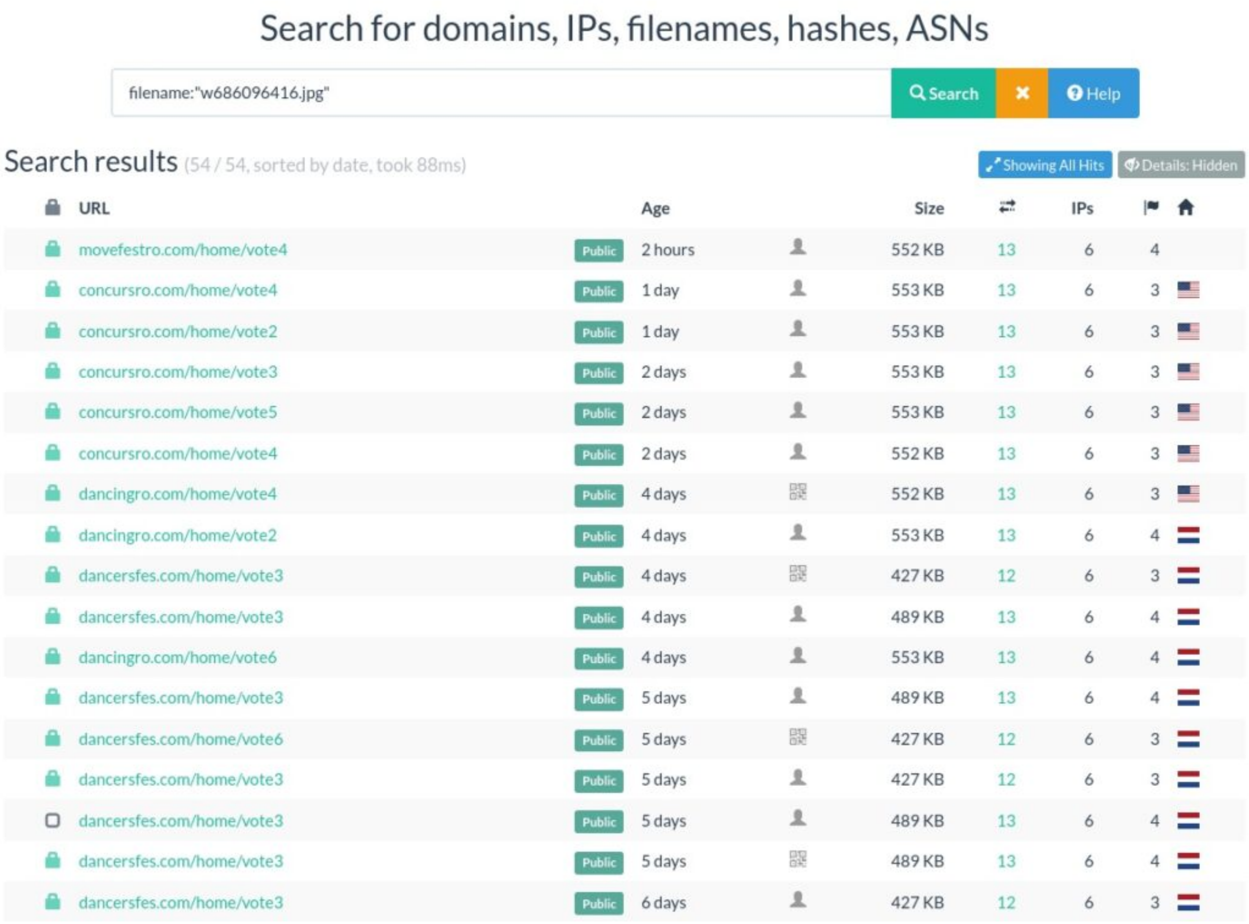
13 HTTP transactions

0 data transactions

Method Protocol	Status	Resource Path		Size x-fer	Time Latency	Type MIME-Type	IP Location
GET H3	200	Primary Request vote4 concursro.com/home/	Show response	14 KB 4 KB	172ms 137ms	Document text/html	172.67.163.171 🇺🇸 CLOUDFLARENET
GET H3	200	integrated.css concursro.com/static/css/		5 KB 2 KB	41ms 40ms	Stylesheet text/css	172.67.163.171 🇺🇸 CLOUDFLARENET
GET H3	200	jquery.js concursro.com/static/js/lib/	Show response	85 KB 32 KB	26ms 25ms	Script application/javascript	172.67.163.171 🇺🇸 CLOUDFLARENET
GET H3	200	sweetalert2.js concursro.com/static/js/lib/	Show response	74 KB 22 KB	55ms 54ms	Script application/javascript	172.67.163.171 🇺🇸 CLOUDFLARENET
GET H3	200	integrated.js concursro.com/static/js/	Show response	995 B 1 KB	55ms 54ms	Script application/javascript	172.67.163.171 🇺🇸 CLOUDFLARENET
GET H3	200	logo.png concursro.com/static/integrated/		27 KB 28 KB	55ms 55ms	Image image/png	172.67.163.171 🇺🇸 CLOUDFLARENET
GET H2	200	noroot.png optim.tildacdn.com/tild6333-3938-4532-a130-316234663630/-/format/webp/		168 KB 168 KB	150ms 43ms	Image image/png	2a03:90c0:41:2801::62 🇩🇪 GCORE G-Core Labs...
GET H2	200	rjgS3Mr2Bz9RfcfMAkF-Kcn4Zth7Xg72LIrAzwlgjLrmF5gJfikmQvXe1Q35mMW1SifelOza4D20XtwcW3jmxPOM.jpg sun9-2.userapi.com/s/v1/ig2/		126 KB 126 KB	149ms 45ms	Image image/jpeg	87.240.185.129 🇷🇺 VKONTAKTE-SPB-AS ...
GET H2	200	css2 fonts.googleapis.com/		17 KB 1 KB	136ms 46ms	Stylesheet text/css	2a00:1450:4001:806::200a 🇩🇪 GOOGLE
GET H2	200	w686096416.jpg i.7fon.org/1000/		63 KB 63 KB	81ms 23ms	Image image/jpeg	213.239.218.106 🇩🇪 HETZNER-AS Hetzne...

Figure 3

We can pivot on the image name and identify other URLs/domains that requested the same image, as displayed below:



Search for domains, IPs, filenames, hashes, ASNs

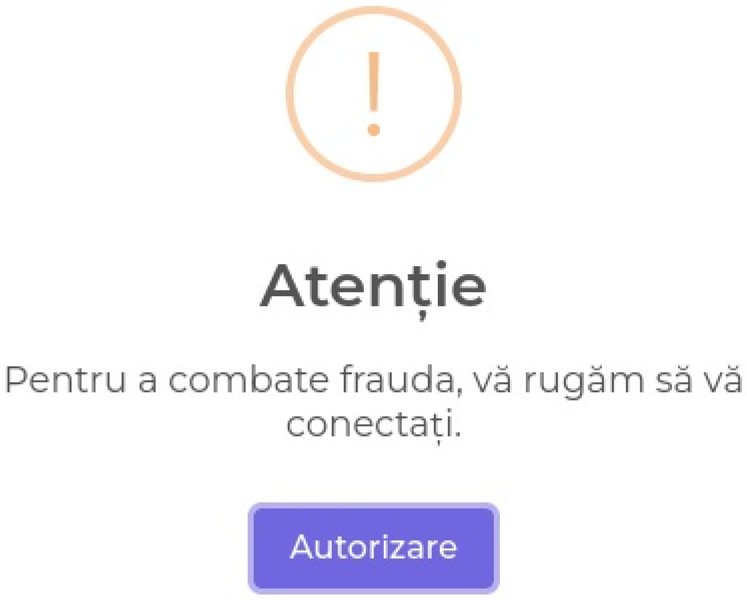
filename:"w686096416.jpg"

Search results (54 / 54, sorted by date, took 88ms)

🔒	URL		Age		Size	⇄	IPs	⚑	🏠
🔒	movefestro.com/home/vote4	Public	2 hours	👤	552 KB	13	6	4	
🔒	concursro.com/home/vote4	Public	1 day	👤	553 KB	13	6	3	🇺🇸
🔒	concursro.com/home/vote2	Public	1 day	👤	553 KB	13	6	3	🇺🇸
🔒	concursro.com/home/vote3	Public	2 days	👤	553 KB	13	6	3	🇺🇸
🔒	concursro.com/home/vote5	Public	2 days	👤	553 KB	13	6	3	🇺🇸
🔒	concursro.com/home/vote4	Public	2 days	👤	552 KB	13	6	3	🇺🇸
🔒	dancingro.com/home/vote4	Public	4 days	▦	552 KB	13	6	3	🇺🇸
🔒	dancingro.com/home/vote2	Public	4 days	👤	553 KB	13	6	4	🇳🇱
🔒	dancersfes.com/home/vote3	Public	4 days	▦	427 KB	12	6	3	🇳🇱
🔒	dancersfes.com/home/vote3	Public	4 days	👤	489 KB	13	6	4	🇳🇱
🔒	dancingro.com/home/vote6	Public	4 days	👤	553 KB	13	6	4	🇳🇱
🔒	dancersfes.com/home/vote3	Public	5 days	👤	489 KB	13	6	4	🇳🇱
🔒	dancersfes.com/home/vote6	Public	5 days	▦	427 KB	12	6	3	🇳🇱
🔒	dancersfes.com/home/vote3	Public	5 days	👤	427 KB	12	6	3	🇳🇱
□	dancersfes.com/home/vote3	Public	5 days	👤	489 KB	13	6	4	🇳🇱
🔒	dancersfes.com/home/vote3	Public	5 days	▦	489 KB	13	6	4	🇳🇱
🔒	dancersfes.com/home/vote3	Public	6 days	👤	427 KB	12	6	3	🇳🇱

Figure 4

When an unsuspecting user clicks on the “Vote” button, the following message, which tells the user to connect in order to “combat fraud”, is displayed:

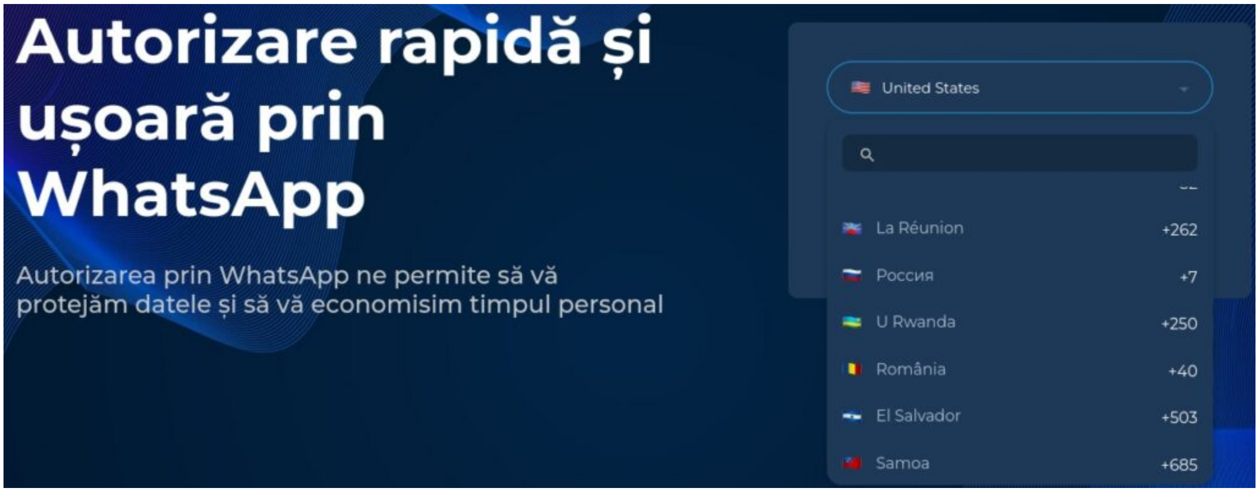


Atenție

Pentru a combate frauda, vă rugăm să vă conectați.

Figure 5

The user should input the WhatsApp number in the box. As we can see below, Russia is written with Cyrillic letters.



Autorizare rapidă și ușoară prin WhatsApp

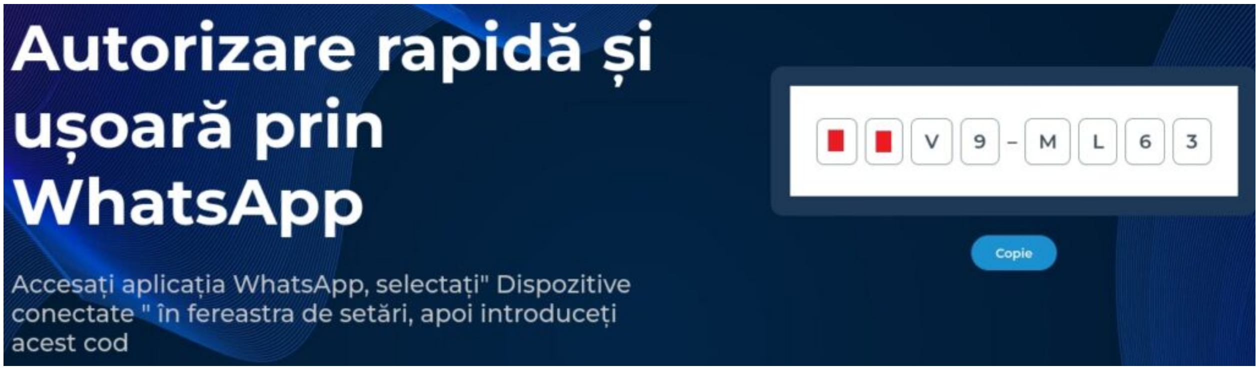
Autorizarea prin WhatsApp ne permite să vă protejăm datele și să vă economisim timpul personal

United States

La Réunion	+262
Россия	+7
U Rwanda	+250
România	+40
El Salvador	+503
Samoa	+685

Figure 6

In this article it is presented the method to link a device with a phone number. The victim needs to enter an 8-character code, which is provided on the suspicious page (see Figure 7). At this stage, the attacker has access to the victim's WhatsApp account.



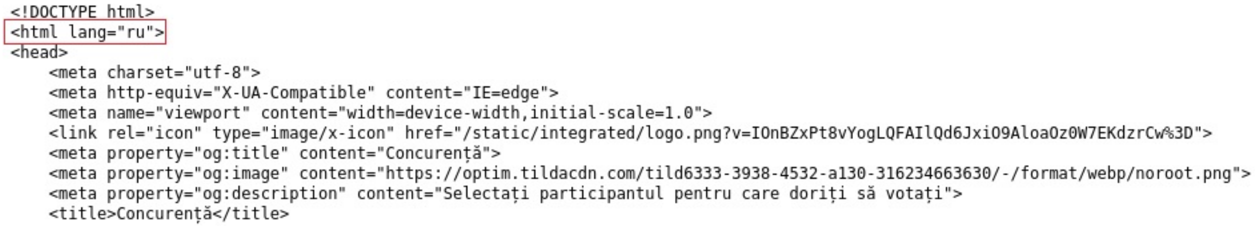
Autorizare rapidă și ușoară prin WhatsApp

[redacted] [redacted] V 9 – M L 6 3

Accesați aplicația WhatsApp, selectați" Dispozitive conectate " în fereastra de setări, apoi introduceți acest cod

Figure 7

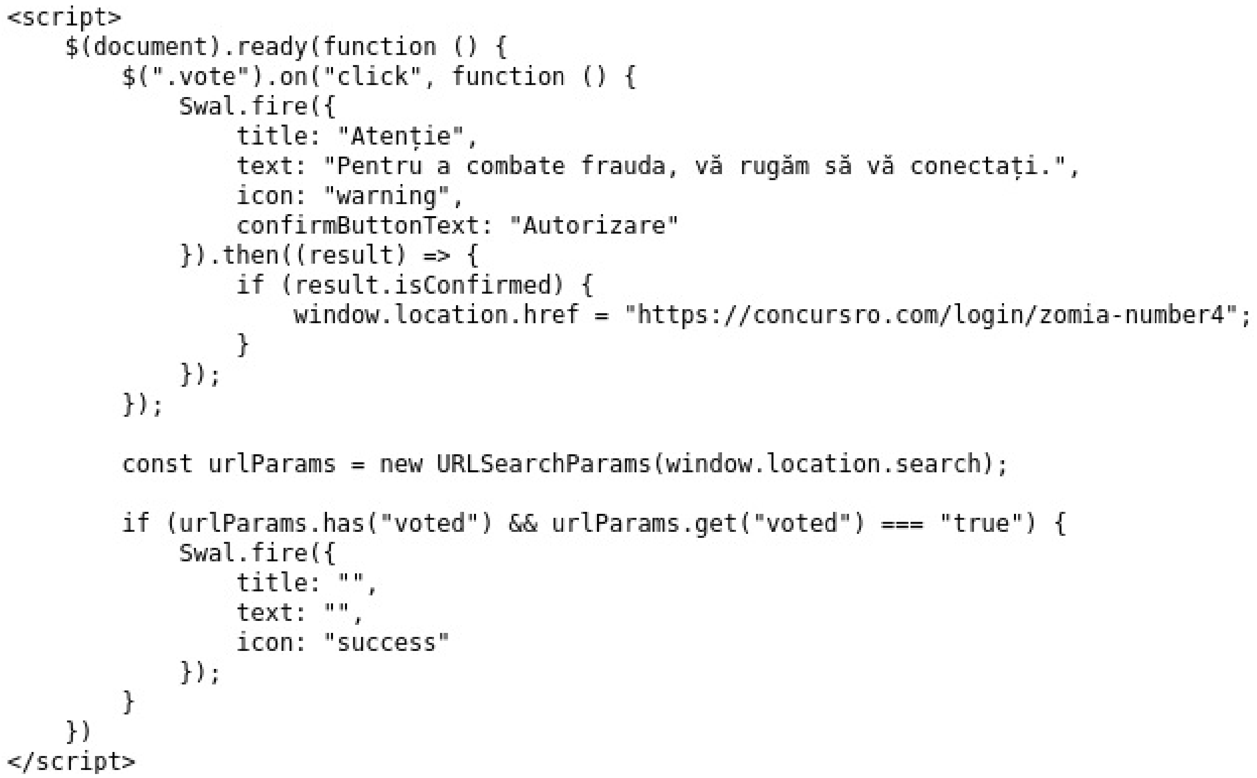
The lang attribute that specifies the language of the content is set to "ru" (Russian language) on the first page:



```
<!DOCTYPE html>
<html lang="ru">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,initial-scale=1.0">
    <link rel="icon" type="image/x-icon" href="/static/integrated/logo.png?v=IOnBZxPt8vYogLQFAIlQd6JxiO9AloaOz0W7EKdzrCw%3D">
    <meta property="og:title" content="Concurență">
    <meta property="og:image" content="https://optim.tildacdn.com/tild6333-3938-4532-a130-316234663630/-/format/webp/noroot.png">
    <meta property="og:description" content="Selectați participantul pentru care doriți să votați">
    <title>Concurență</title>
```

Figure 8

The script responsible for handling the "authorization" can be found on the same domain at "/login/zomia-number4":



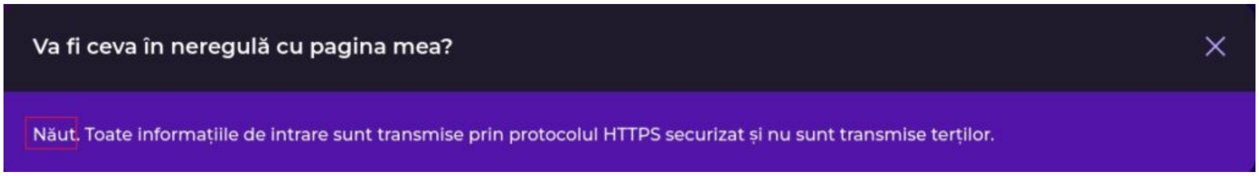
```
<script>
    $(document).ready(function () {
        $(".vote").on("click", function () {
            Swal.fire({
                title: "Atenție",
                text: "Pentru a combate frauda, vă rugăm să vă conectați.",
                icon: "warning",
                confirmButtonText: "Autorizare"
            }).then((result) => {
                if (result.isConfirmed) {
                    window.location.href = "https://concursro.com/login/zomia-number4";
                }
            });
        });

        const urlParams = new URLSearchParams(window.location.search);

        if (urlParams.has("voted") && urlParams.get("voted") === "true") {
            Swal.fire({
                title: "",
                text: "",
                icon: "success"
            });
        }
    })
</script>
```

Figure 9

Some sections on the suspicious page contain Broken Romanian that should raise suspicion:



Va fi ceva în neregulă cu pagina mea?

Năut. Toate informațiile de intrare sunt transmise prin protocolul HTTPS securizat și nu sunt transmise terților.

Figure 10

We’ve identified the following domains part of this campaign:

concursro[.]com
dancingro[.]com
dancersfes[.]com
rocondance[.]com
rodancee[.]com
rofesting[.]com
danccingro[.]com
rodaciing[.]com
dancerofest[.]com
danciingro[.]com
rodancehit[.]com
rodancing[.]com
rodence[.]com

dancechoise[.]com
festdance[.]com
coonnkurenta[.]top
concursdedans[.]com
concursiarna[.]com
dancersro[.]com
dancingvot[.]top
showdance[.]top
votingdance[.]top
dancevotr[.]top
dancefesting[.]top
feastdance[.]top
danceiivot[.]top

Based on pivoting on another resource, we could determine that the attacker targeted English and Turkish speaking users in the past:

- https[:]//starsdance[.]top/home/vote32 – English page
- https[:]//starsdance[.]top/home/vote101 – Turkish page

The threat actor has access to the victim’s WhatsApp account after entering the 8-character code and continues to send the same voting message to his/her contacts. As a consequence, the victim might lose the WhatsApp account because of spamming, as reported by multiple people on Reddit.

We advise users to not enter 8-character codes from dubious websites to access their WhatsApp account. We will continue monitoring the campaign and update the blog post if necessary.