

Autor: Dominik Topolski

Spis Treści:

|  |           |
|--|-----------|
| <b>Pierwsze zagrożenie - euro-paczka</b> | <b>1</b>  |
| <b>Drugie zagrożenie - cocina bien</b>   | <b>8</b>  |
| <b>Trzecie zagrożenie - hovarokosak</b>  | <b>13</b> |

## Pierwsze zagrożenie - euro-paczka

hxxps://euro-paczka.cloud/RNhd129BmmrUGOmc4uG/1eirNo

### 1. Czy pod wskazanym adresem obecnie lub w przeszłości znajdowały się jakieś niebezpieczne treści?

Tak. Następujący dostawcy rozwiązań z zakresu bezpieczeństwa wskazali ten adres jako złośliwy/phishing:

[VirusTotal](#):

|                         |             |                  |             |
|-------------------------|-------------|------------------|-------------|
| alphaMountain.ai        | ⚠ Phishing  | AlphaSOC         | ⚠ Phishing  |
| Avira                   | ⚠ Phishing  | BitDefender      | ⚠ Malware   |
| Certego                 | ⚠ Phishing  | Cluster25        | ⚠ Phishing  |
| CyRadar                 | ⚠ Malicious | ESET             | ⚠ Phishing  |
| Forcepoint ThreatSeeker | ⚠ Phishing  | Fortinet         | ⚠ Phishing  |
| G-Data                  | ⚠ Malware   | Heimdal Security | ⚠ Phishing  |
| Kaspersky               | ⚠ Phishing  | Lionic           | ⚠ Phishing  |
| Phishing Database       | ⚠ Phishing  | Phishtank        | ⚠ Phishing  |
| Seclookup               | ⚠ Malicious | SOCRadar         | ⚠ Malware   |
| Sophos                  | ⚠ Phishing  | VIPRE            | ⚠ Malicious |
| Webroot                 | ⚠ Malicious |                  |             |

---

## Categories

---

|                         |  |
|-------------------------|--|
| Forcepoint ThreatSeeker | <a href="#">Forcepoint ThreatSeeker</a><br>phishing and other frauds |
| Sophos                  | <a href="#">Sophos</a><br>phishing and fraud                         |
| Webroot                 | <a href="#">Webroot</a><br>Phishing and Other Frauds                 |

---

## History

---

|                  |                         |
|------------------|-------------------------|
| First Submission | 2023-10-15 19:33:24 UTC |
| Last Submission  | 2023-10-22 17:53:16 UTC |
| Last Analysis    | 2023-10-22 17:53:16 UTC |

---

## HTTP Response

---

### Final URL

<https://euro-paczka.cloud/RNhd129BmmrUGOmc4uG/1eirNo>

### Serving IP Address

172.67.160.109

### Status Code

200








### Body Length

12.85 KB

### Body SHA-256

1b595e270109ce230a016af072493fa1e31cc2c6c0dc306aa9a9567fc863f834

[Urlvoid.com](https://urlvoid.com):

| Engine  | Result     |
|---|------------|
|  Avira       | ✖ Detected |
|  BitDefender | ✖ Detected |
|  CERT Polska | ✖ Detected |
|  Fortinet    | ✖ Detected |
|  PhishTank   | ✖ Detected |
|  SURBL       | ✖ Detected |
|  Seclookup  | ✖ Detected |

Strona podpisuje się certyfikatem cert.pl prawdopodobnie przez znajdujący się na niej alert CERT, co sprawia, że dodatkowo jest blokowana przez niepasujący certyfikat.

Error code: SSL\_ERROR\_BAD\_CERT\_DOMAIN

#### **a. jeżeli tak to ustalenie kto potencjalnie był ich celem oraz czego dotyczyły?**

Wnioskując po nazwie, ten adres mógł podszywać się pod europaczka.pl lub euro-paka.pl i wyludzać dane do logowania użytkowników tych stron.

## **2. Czy wskazany adres jest częścią jakiejś innych kampanii lub ich kontynuacją?**

Wskazany adres mógł być powiązany z podobną kampanią:

<https://cert.pl/posts/2022/04/flubot-smishing/>

W tej kampanii ofiara otrzymuje wiadomość SMS z prośbą o dopłatę oraz link.

Jak można przeczytać w artykule:

<https://www.bgk.pl/bankowosc-i-serwisy/cyberbezpieczenstwo/co-zrobic-gdy-dostalem-sms-a-od-firmy-kurierskiej-z-prosba-o-doplate/>

“Link w takim SMS-ie prowadzi najczęściej do fałszywej strony internetowej, za pośrednictwem której przestępcy wymuszają podanie danych wrażliwych lub pobranie złośliwej aplikacji.”

### **3. Czy wskazany adres znajduje się na jakiś czarnych listach?**

[Quad9](#) podaje następujących dostawców informacji o zagrożeniach, którzy umieścili tę domenę na czarnej liście:

- ▶ GCA-DOMAINTRUST
- ▶ CERT Polska

Skan Spiderfoot wskazał także te czarne listy jako zawierające euro-paczka.cloud:

1. CleanBrowsing DNS - Security
2. Comodo Secure DNS
3. DNS for Family
4. OpenDNS
5. SURBL
6. Steven Black Hosts Blacklist

#### 4. Informacje o samych domenach i miejscu ich hostowania obecnie i w przeszłości

[who.is](https://who.is) (Duża część informacji o tej domenie jest niedostępne ze względu na ustawienia prywatności):

| Registrar Info            |   |
|---------------------------|---|
| Name                      | NAMECHEAP   |
| Whois Server              | whois.namecheap.com   |
| Referral URL              | https://www.namecheap.com   |
| Status                    | addPeriod https://icann.org/epp#addPeriod<br>clientHold https://icann.org/epp#clientHold<br>clientTransferProhibited https://icann.org/epp#clientTransferProhibited |
| Important Dates           |   |
| Expires On                | 2024-10-15  |
| Registered On             | 2023-10-15  |
| Updated On                | 2023-10-15  |
| Name Servers              |   |
| carioca.ns.cloudflare.com | 162.159.38.20   |
| kellen.ns.cloudflare.com  | 172.64.35.160   |

Country: IS (Iceland)

Site status: Inactive

| DNS Records for euro-paczka.cloudnrhd129bmmrugomc4ug1eirno |      |       |          |  |
|--|------|-------|----------|--|
| Hostname   | Type | TTL   | Priority | Content  |
| euro-paczka.cloudnrhd129bmmrugomc4ug1eirno                 | SOA  | 86399 |          | a.root-servers.net nstld@verisign-grs.com 2023102000 1800 900 604800 86400 |

## Linux whois:

```

(kali@kali)~$ whois euro-paczka.cloud --verbose
Using server whois.nic.cloud.
Query string: "euro-paczka.cloud"

Domain Name: euro-paczka.cloud
Registry Domain ID: D0-eued4d538e5574944dabf5a9dd6e22e6-ARUBA
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://www.namecheap.com
Updated Date: 2023-10-15T20:14:46.014Z
Creation Date: 2023-10-15T14:34:42.083Z
Registry Expiry Date: 2024-10-15T14:34:42.083Z
Registrar: NAMECHEAP
Registrar IANA ID: 1068
Registrar Abuse Contact Email: support@namecheap.com
Registrar Abuse Contact Phone: +1.3102593259
Domain Status: clientHold https://icann.org/epp#clientHold
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Capital Region
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IS
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Billing ID: REDACTED FOR PRIVACY
Billing Name: REDACTED FOR PRIVACY
```

```

Billing Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: carioca.ns.cloudflare.com
Name Server: kellen.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN RDNS Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of WHOIS database: 2023-10-20T12:41:21.247Z <<<

For more information on domain status codes, please visit https://icann.org/epp

The WHOIS information provided in this page has been redacted
in compliance with ICANN's Temporary Specification for gTLD
Registration Data.

The data in this record is provided by Uniregistry for informational
purposes only, and it does not guarantee its accuracy. Uniregistry is
authoritative for whois information in top-level domains it operates
under contract with the Internet Corporation for Assigned Names and
Numbers. Whois information from other top-level domains is provided by
a third-party under license to Uniregistry.

This service is intended only for query-based access. By using this
service, you agree that you will use any data presented only for lawful
purposes and that, under no circumstances will you use (a) data
acquired for the purpose of allowing, enabling, or otherwise supporting
the transmission by e-mail, telephone, facsimile or other
communications mechanism of mass unsolicited, commercial advertising
or solicitations to entities other than your existing customers; or
(b) this service to enable high volume, automated, electronic processes
that send queries or data to the systems of any Registrar or any
Registry except as reasonably necessary to register domain names or
modify existing domain name registrations.

Uniregistry reserves the right to modify these terms at any time. By
submitting this query, you agree to abide by this policy. All rights
reserved.
```

Linux dig:

```
(kali㉿kali)-[~]  
$ dig euro-paczka.cloud ANY  
  
; <<>> DiG 9.18.12-1-Debian <<>> euro-paczka.cloud ANY  
;; global options: +cmd  
;; Got answer:  
;; —>HEADER<— opcode: QUERY, status: NOERROR, id: 40640  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
euro-paczka.cloud.          IN      ANY  
  
;; ANSWER SECTION:  
euro-paczka.cloud.      86344   IN      A      195.187.6.33  
  
;; Query time: 3 msec  
;; SERVER: 212.75.96.2#53(212.75.96.2) (TCP)  
;; WHEN: Thu Oct 19 18:28:27 CEST 2023  
;; MSG SIZE rcvd: 62
```

Linux getent:

```
(kali㉿kali)-[~]  
$ getent hosts euro-paczka.cloud  
195.187.6.33      euro-paczka.cloud
```

## Drugie zagrożenie - cocina bien

hxxps://cocinabien.es/

### 1. Czy pod wskazanym adresem obecnie lub w przeszłości znajdowały się jakieś niebezpieczne treści?

Tak. Następujący dostawcy rozwiązań z zakresu bezpieczeństwa wskazali ten adres jako złośliwy/ phishing:

#### Virustotal:

|                  |             |             |             |
|------------------|-------------|-------------|-------------|
| alphaMountain.ai | ⚠ Phishing  | AlphaSOC    | ⚠ Phishing  |
| Avira            | ⚠ Phishing  | BitDefender | ⚠ Phishing  |
| Cluster25        | ⚠ Phishing  | CRDF        | ⚠ Malicious |
| CyRadar          | ⚠ Malicious | ESET        | ⚠ Phishing  |
| Fortinet         | ⚠ Phishing  | G-Data      | ⚠ Phishing  |
| Kaspersky        | ⚠ Phishing  | Seclookup   | ⚠ Malicious |
| SOCRadar         | ⚠ Phishing  | Sophos      | ⚠ Phishing  |
| VIPRE            | ⚠ Malicious | Webroot     | ⚠ Malicious |



## Categories ⓘ

|                       |   |
|-----------------------|---|
| Webroot               | <a href="#">Webroot</a><br>Phishing and Other Frauds                                    |
| Sophos                | <a href="#">Sophos</a><br>phishing and fraud  |
| Xcitium Verdict Cloud | <a href="#">Xcitium Verdict Cloud</a><br>media sharing                                  |
| alphaMountain.ai      | <a href="#">alphaMountain.ai</a><br>Phishing, Scam/Illegal/Unethical (alphaMountain.ai) |

## History ⓘ

|                  |                         |
|------------------|-------------------------|
| First Submission | 2023-10-03 22:34:54 UTC |
| Last Submission  | 2023-10-19 14:52:44 UTC |
| Last Analysis    | 2023-10-19 14:52:44 UTC |

## HTTP Response ⓘ

### Final URL

<https://cocinabien.es/>

### Serving IP Address

217.160.0.116

### Status Code

403

### Body Length

1.24 KB

### Body SHA-256

f183d5dbf5ade60dba3ac344ce47de08e3efb7476f4cc5330c923c0100f2ac7d

[urlvoid:](#)

 **Avira**

✖ Detected

 **BitDefender**

✖ Detected

 **CERT Polska**

✖ Detected

 **CRDF**

✖ Detected

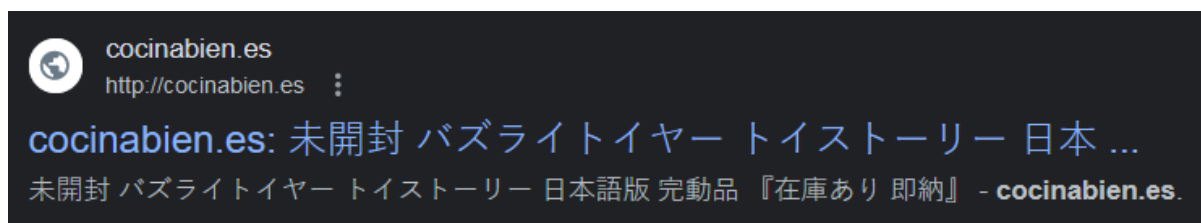
 **Fortinet**

✖ Detected

 **Seclookup**

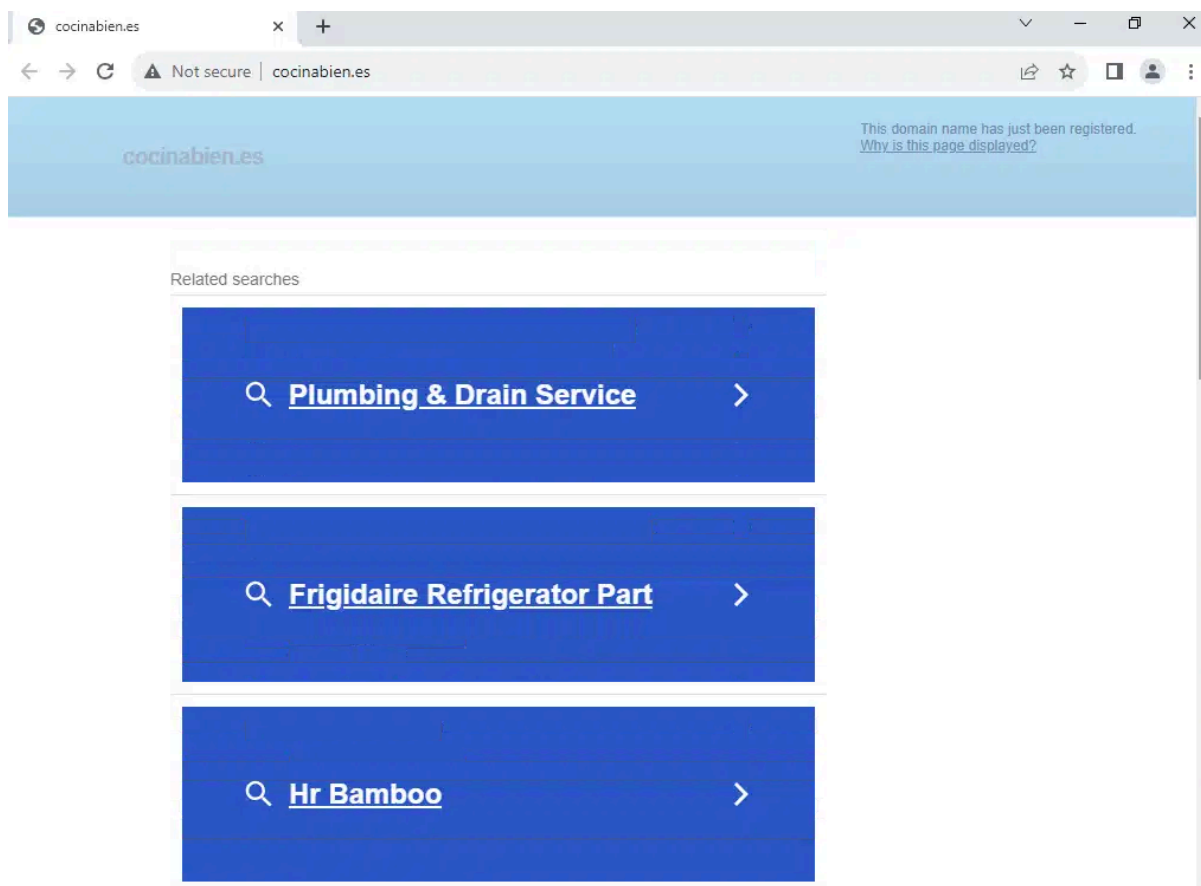
✖ Detected

a. jeżeli tak to ustalenie kto potencjalnie był ich celem oraz czego dotyczyły?



Sądząc po nazwie ta strona mogła być w przeszłości hiszpańskim portalem kucharskim co okazuje się być prawdą patrząc na zarchiwizowaną wersję tej strony z 2018 r. (<https://web.archive.org/web/20180828202033/https://cocinabien.es/>), ale obecnie reklamuje sprzedaż zabawek po japońsku (z japońskiego: Nieotwarta japońska wersja Buzz Lightyear Toy Story w świetnym stanie „W magazynie i gotowa do wysyłki”).

Strona w sandboxie browserling.com. Obecnie strona nie zawiera wcześniej widniejących tam treści:



Możliwe powody takiej sytuacji to między innymi:

1. Rebranding
2. Wygaśnięcie domeny
3. Atak hakerski

## **2. Czy wskazany adres jest częścią jakiejś innych kampanii lub ich kontynuacją?**

Możliwe powiązanie z fałszywymi sklepami. Jednakże, nie można jednoznacznie stwierdzić czy strona jest powiązana z fałszywymi sklepami czy po prostu wygaśła.

<https://cert.pl/falszywe-sklepy/>

## **3. Czy wskazany adres znajduje się na jakiś czarnych listach?**

[Quad9](#) podaje następujących dostawców informacji o zagrożeniach, którzy umieścili tę domenę na czarnej liście:

- ▶ GCA-DOMAINTRUST
- ▶ CERT Polska

Skan Spiderfoot wskazał także te listy jako zawierające cocinabien.es:

1. CleanBrowsing DNS - Security
2. Comodo Secure DNS
3. DNS for Family
4. OpenDNS - Phishing
5. Steven Black Hosts Blocklist

#### 4. Informacje o samych domenach i miejscu ich hostowania obecnie i w przeszłości

Informacje o tym adresie na hiszpańskiej stronie o dominios.es

| REGISTRANT DATA               |                      |  |
|-------------------------------|----------------------|--|
| Domain name                   | cocinabien.es        |  |
| state                         | Activated            |  |
| Identifier                    | 21A56C-ESNIC-F5      |  |
| Registrant                    | Julio Bascaran Mesa  |  |
| Register Date                 | 01-03-2011           |  |
| Date of renovation            | 01-03-2024           |  |
| Registrar                     | 1&1 IONOS            |  |
| ADMINISTRATIVE CONTACT PERSON |                      |  |
| Identifier                    | 21A56C-ESNIC-F5      |  |
| TECHNICAL CONTACT PERSON      |                      |  |
| Identifier                    | 2A7DD0-ESNIC-F5      |  |
| Name                          | Hostmaster ONEANDONE |  |
| INVOICING CONTACT PERSON      |                      |  |
| DNS SERVERS                   |                      |  |
| Server Name                   | IP                   |  |
| ns1055.ui-dns.com             |                      |  |
| ns1033.ui-dns.de              |                      |  |
| ns1117.ui-dns.org             |                      |  |
| ns1124.ui-dns.biz             |                      |  |

Hostingchecker.com

To find out where a website is hosted enter the URL address:

cocinabien.es

FIND HOST

It is hosted by: **IONOS SE**

WHOIS information: [Click here](#)

Organization name: **Ionos**

IP address: **217.160.0.116**

AS(autonomous system) number and organization: **AS8560 IONOS SE**

AS name: **IONOS-AS**

Reverse DNS of the IP: **217-160-0-116.elastic-ssl.ui-r.com**

City: **Essen**

Country: **Germany**

Visit HostGator

Linux whois:

This TLD has no whois server, but you can access the whois database at  
<https://www.nic.es/>

Linux dig:

```
(kali㉿kali)-[~]
$ dig cocinabien.es

; <<>> DiG 9.18.12-1-Debian <<>> cocinabien.es
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 53968
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
cocinabien.es.                IN      A

;; ANSWER SECTION:
cocinabien.es.                53534   IN      A      195.187.6.33

;; Query time: 4 msec
;; SERVER: 212.75.96.2#53(212.75.96.2) (UDP)
;; WHEN: Sat Oct 21 22:15:56 CEST 2023
;; MSG SIZE rcvd: 58

IDSweep.sh
```

Linux getent:

```
(kali㉿kali)-[~]
$ getent hosts cocinabien.es
195.187.6.33      cocinabien.es
```

## Trzecie zagrożenie - hovarokosak

hxxps://hovarokosak.com/ndjs4Hkd?utm\_campaign=aua309orlspad1&utm\_source=ORLEN&utm\_content=aua309orlspad1&pixel=354431829978209&id\_buyer=80&gi=629

### 1. Czy pod wskazanym adresem obecnie lub w przeszłości znajdowały się jakieś niebezpieczne treści?

Tak. Następujący dostawcy rozwiązań z zakresu bezpieczeństwa wskazali ten adres jako złośliwy/ phishing:

[VirusTotal](#):

|                  |             |             |             |
|------------------|-------------|-------------|-------------|
| alphaMountain.ai | ⚠ Phishing  | AlphaSOC    | ⚠ Phishing  |
| Avira            | ⚠ Phishing  | BitDefender | ⚠ Phishing  |
| Cluster25        | ⚠ Phishing  | CRDF        | ⚠ Malicious |
| CyRadar          | ⚠ Malicious | ESET        | ⚠ Phishing  |
| Fortinet         | ⚠ Phishing  | G-Data      | ⚠ Phishing  |
| Kaspersky        | ⚠ Phishing  | Seclookup   | ⚠ Malicious |
| SOCRadar         | ⚠ Phishing  | Sophos      | ⚠ Malware   |
| VIPRE            | ⚠ Malicious | Webroot     | ⚠ Malicious |



## Categories ①

|                         |  |
|-------------------------|--|
| Forcepoint ThreatSeeker | <a href="#">Forcepoint ThreatSeeker</a><br>newly registered websites       |
| Sophos                  | <a href="#">Sophos</a><br>spyware and malware                              |
| Webroot                 | <a href="#">Webroot</a><br>Phishing and Other Frauds                       |
| alphaMountain.ai        | <a href="#">alphaMountain.ai</a><br>Malicious, Phishing (alphaMountain.ai) |

## History ①

|                  |                         |
|------------------|-------------------------|
| First Submission | 2023-10-05 00:10:39 UTC |
| Last Submission  | 2023-10-21 20:25:52 UTC |
| Last Analysis    | 2023-10-21 20:25:52 UTC |

## HTTP Response ①

### Final URL

<https://hovarokosak.com/>

### Serving IP Address

172.67.150.246

### Status Code

404

### Body Length

13 B

### Body SHA-256

7d04f7431bbfa41a04bcc7e6b98b9de0d919756c4c671c5785c99fff45f16402

[Urlvoid:](#)

 **Avira**

✖ Detected

 **BitDefender**

✖ Detected

 **CERT Polska**


✖ Detected

 **CRDF**

✖ Detected

 **Fortinet**

✖ Detected

 **PhishStats**

✖ Detected

 **PhishTank**

✖ Detected

 **Seclookup**

✖ Detected

## a. jeżeli tak to ustalenie kto potencjalnie był ich celem oraz czego dotyczyły?

Podany link jest długi więc prawdopodobnie warto go przeanalizować:

1. [hovarokosak.com](http://hovarokosak.com) - domena internetowa
2. [/ndjs4Hkd](#) - to może być identyfikator ścieżki lub podstrona na witrynie. Jednak w tym kontekście jest to prawdopodobnie używane jako unikalny identyfikator sesji lub do celów śledzenia.
3. [?utm\\_campaign=aua309orlspad1&utm\\_source=ORLEN&utm\\_content=aua309orlspad1&pixel=354431829978209&id\\_buyer=80&gi=629](http://?utm_campaign=aua309orlspad1&utm_source=ORLEN&utm_content=aua309orlspad1&pixel=354431829978209&id_buyer=80&gi=629) - to jest część linku, która zawiera parametry śledzenia i informacje analityczne.
  - o [utm\\_campaign](#) - To jest identyfikator kampanii marketingowej.
  - o [utm\\_source](#) - Wskazuje źródło, z którego link został kliknięty, w tym przypadku "ORLEN".
  - o [utm\\_content](#) - Oznacza zawartość lub konkretne ogłoszenie, które przekierowało użytkownika.
  - o [pixel](#) - To może być identyfikator piksela lub narzędzia do śledzenia.
  - o [id\\_buyer](#) - To jest prawdopodobnie identyfikator użytkownika lub kupującego.
  - o [gi](#) - To może być inny identyfikator związanego z kampanią lub użytkownikiem.

Strona w sandboxie browserling.com:



Document x +

hovarokosak.com/ndjs4Hkd?utm\_campaign=aua309orlspad1&utm\_source=ORLEN&utm\_content=aua...

## Investment Advisory Course and Investment Project Evaluation

Sie fragen sich, wo Sie sicher investieren können? Wählen Sie aus unserer Datenbank einen Kurs über grundlegende und fortgeschrittene Techniken zur Bewertung der Rentabilität von Investitionen und erfahren Sie, wo Sie sicher investieren können. In unserer Datenbank finden Sie Informationen darüber, welche Risiken mit Investitionen in Gold verbunden sind, wie Investitionen an der Börse funktionieren und was alternative Investitionen sind und ob es sich lohnt, in Anleihen zu investieren.

Planen Sie den Kauf einer Wohnung zur Vermietung? Erfahren Sie die Geheimnisse des Immobilieninvestments und lernen Sie, in Immobilien zu investieren. Erfahren Sie, worauf Sie bei der Auswahl von Wohnungsbaudarlehen achten sollten, und lernen Sie, Investitionsprojekte zu bewerten und ihre Rendite, ROI und ROE zu beurteilen.

Sie beginnen gerade erst mit dem Investieren, aber Sie spüren, dass Sie sich beruflich damit beschäftigen möchten? Informieren Sie sich über qualifizierte Berufskurse und werden Sie zertifizierter Investmentberater. Lernen Sie, wie Sie Investmentportfolios basierend auf den Bedürfnissen von Unternehmen und Privatpersonen empfehlen können.

Sind Sie im Bereich Investmentberatung tätig oder entwickeln Sie Ihr eigenes Unternehmen? Informieren Sie sich über die neuesten Entwicklungen in Bezug auf sichere und rentable Geldanlagen sowie Trends im Bereich der Personalinvestitionen.

Email

Tekst po przetłumaczeniu na j. polski:

“Zastanawiasz się gdzie możesz bezpiecznie inwestować? Wybierz z naszej bazy kurs dotyczący technik podstawowych i zaawansowanych Oceń opłacalność inwestycji i dowiedz się, gdzie możesz bezpiecznie inwestować. W naszej bazie znajdziesz informacje o: jakie ryzyko wiąże się z inwestowaniem w złoto, jak działają inwestycje na giełdzie oraz

jakie są inwestycje alternatywne i czy warto inwestować w obligacje. Planujesz zakup mieszkania na wynajem? Poznaj tajniki inwestowania w nieruchomości i ucz się; inwestować w nieruchomości. Dowiedz się, na co zwrócić uwagę przy wyborze kredytu mieszkaniowego i dowiedz się, jak oceniać projekty inwestycyjne i oceniać ich zwrot, ROI i ROE. Dopiero zaczynasz inwestować, ale czujesz, że chcesz zajmować się tym profesjonalnie? Skorzystaj z kwalifikowanych kursów zawodowych i zostań certyfikowanym doradcą inwestycyjnym. Dowiedz się, jak rekomendować portfele inwestycyjne w oparciu o potrzeby firm i osób prywatnych. Prowadzisz działalność w obszarze doradztwa inwestycyjnego lub rozwijasz własną firmę? Poznaj najnowsze osiągnięcia w zakresie bezpiecznych i zyskowych inwestycji oraz trendy w inwestycjach personalnych.”

Sądząc po obecności `utm_source=ORLEN` w linku, ta strona prawdopodobnie wyświetlała się ludziom klikającym w reklamę inwestycji w Orlen tzw. Oszustwo na Orlen.

## **2. Czy wskazany adres jest częścią jakiejś innych kampanii lub ich kontynuacją?**

W linku jest nazwa “ORLEN”. Możliwe jest, że strona była częścią oszustwa związanego z zachęcaniem Polaków do inwestowania w biznes energetyczny. W tej kampanii wykorzystano wizerunek prezesa Orlenu Daniela Obajtka, prezydenta RP Andrzeja Dudy i innych znanych osób. Rok temu o tej sprawie pisał serwis CyberDefence24:

<https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-internetowe-oszustwo-na-prezydenta-premiera-i-pkn-orken-to-scam>

<https://cert.pl/posts/2022/04/falszywe-inwestycje/>

## **3. Czy wskazany adres znajduje się na jakiś czarnych listach?**

[Quad9](#) podaje następujących dostawców informacji o zagrożeniach, którzy umieścili tę domenę na czarnej liście:

► CERT Polska

Skan Spiderfoot wskazał także te czarne listy jako zawierające euro-paczka.cloud:

1. CleanBrowsing DNS - Security
2. CloudFlare - Malware
3. Comodo Secure DNS
4. DNS for Family
5. Quad9
6. Steven Black Hosts Blocklist

#### 4. Informacje o samych domenach i miejscu ich hostowania obecnie i w przeszłości

whoisdatacenter.org

## HOVAROKOSAK.COM

|                         |                        |
|-------------------------|------------------------|
| Domain Name             | hovarokosak.com        |
| Domain Registered On    | 02-10-2023             |
| Domain Expiry Date      | 02-10-2024             |
| Registrant Name         | Igor Sisimisi          |
| Registrant Company Name | IgorSisimisi           |
| Registrant Address      |                        |
| Registrant Country      | Ukraine                |
| Registrant Email        | igorsisimisi@gmail.com |
| Registrant Phone        | 380999434233           |

To samo nazwisko "Igor Sisimisi" można znaleźć wśród informacji o stronie <https://who.is/whois/balticpipeess.site>. Baltic Pipe to oszustwo bardzo podobne do omawianego Orlenu. Tu również oszuści namawiali do inwestycji obiecując wysokie gwarantowane dochody. Więcej na stronie:

[https://demagog.org.pl/fake\\_news/zakup-akcji-baltic-pipe-uwaga-na-internetowe-oszustwa/](https://demagog.org.pl/fake_news/zakup-akcji-baltic-pipe-uwaga-na-internetowe-oszustwa/)

Linux whois

```
(kali@kali)-[~]
$ whois hovarokosak.com
Domain Name: HOVAROKOSAK.COM
Registry Domain ID: 2818666631_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2023-10-02T12:15:27Z
Creation Date: 2023-10-02T12:15:27Z
Registry Expiry Date: 2024-10-02T12:15:27Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: GIANCARLO.NS.CLOUDFLARE.COM
Name Server: SHARON.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-10-22T17:48:51Z <<<
```

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.  
Domain Name: HOVAROKOSAK.COM  
Registry Domain ID: 2818666631\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.publicdomainregistry.com  
Registrar URL: www.publicdomainregistry.com  
Updated Date: 2023-10-02T12:15:28Z  
Creation Date: 2023-10-02T12:15:27Z  
Registrar Registration Expiration Date: 2024-10-02T12:15:27Z  
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com  
Registrar IANA ID: 303  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Registry Registrant ID: Not Available From Registry  
Registrant Name: Igor Sisimisi  
Registrant Organization: IgorSisimisi  
Registrant Street: st. Solomianska, 90  
Registrant City: Zaporizhzhya  
Registrant State/Province: Zaporizhia Oblast  
Registrant Postal Code: 69096  
Registrant Country: UA  
Registrant Phone: +380.999434233  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: igorsisimisi@gmail.com  
Registry Admin ID: Not Available From Registry  
Admin Name: Igor Sisimisi  
Admin Organization: IgorSisimisi  
Admin Street: st. Solomianska, 90  
Admin City: Zaporizhzhya  
Admin State/Province: Zaporizhia Oblast  
Admin Postal Code: 69096  
Admin Country: UA  
Admin Phone: +380.999434233  
Admin Phone Ext:  
Admin Fax:  
Admin Fax Ext:  
Admin Email: igorsisimisi@gmail.com  
Registry Tech ID: Not Available From Registry  
Tech Name: Igor Sisimisi  
Tech Organization: IgorSisimisi  
Tech Street: st. Solomianska, 90  
Tech City: Zaporizhzhya  
Tech State/Province: Zaporizhia Oblast  
Tech Postal Code: 69096  
Tech Country: UA  
Tech Phone: +380.999434233  
Tech Phone Ext:  
Tech Fax:  
Tech Fax Ext:  
Tech Email: igorsisimisi@gmail.com

Name Server: giancarlo.ns.cloudflare.com  
Name Server: sharon.ns.cloudflare.com  
DNSSEC: Unsigned  
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com  
Registrar Abuse Contact Phone: +1.2013775952  
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>  
>>> Last update of WHOIS database: 2023-10-22T17:49:00Z <<<

For more information on Whois status codes, please visit <https://icann.org/epp>

Registration Service Provided By: IGORSISIMISI

## Linux dig

```
(kali㉿kali)-[~]  
$ dig hovarokosak.com  
  
; <<>> DiG 9.18.12-1-Debian <<>> hovarokosak.com  
;; global options: +cmd  
;; Got answer:  
;; —>HEADER<— opcode: QUERY, status: NOERROR, id: 32287  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags;; udp: 512  
;; QUESTION SECTION:  
hovarokosak.com.                IN      A  
  
;; ANSWER SECTION:  
hovarokosak.com.                86400   IN      A      195.187.6.33  
  
;; Query time: 8 msec  
;; SERVER: 212.75.96.2#53(212.75.96.2) (UDP)  
;; WHEN: Sun Oct 22 19:51:45 CEST 2023  
;; MSG SIZE rcvd: 60
```

## Linux getent

```
(kali㉿kali)-[~]  
$ getent hosts hovarokosak.com  
195.187.6.33      hovarokosak.com
```

Autor: Dominik Topolski