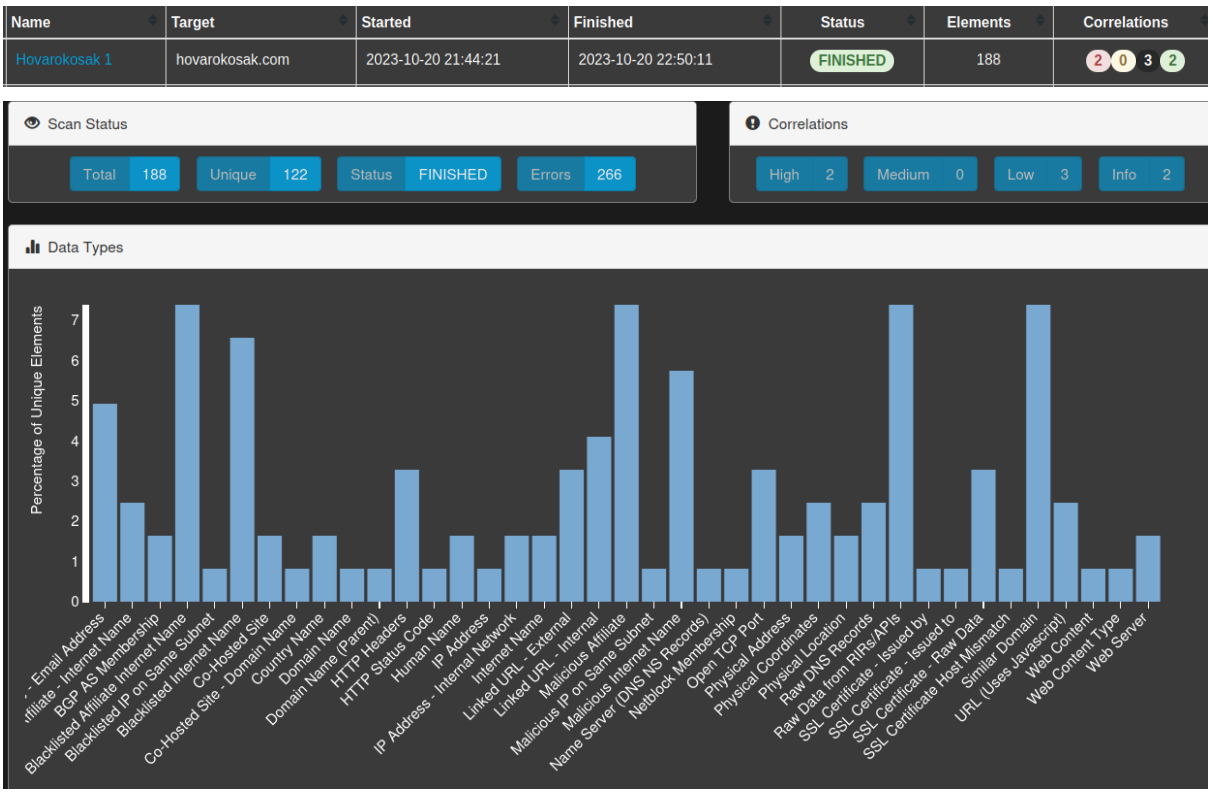
SpiderFoot analysis of hovarokosak.com

SpiderFoot to narzędzie do automatyzacji wywiadu typu open source (OSINT). Integruje się z niemal każdym dostępnym źródłem danych i wykorzystuje szereg metod analizy danych, dzięki czemu nawigacja po nich jest łatwa. SpiderFoot ma wbudowany serwer sieciowy zapewniający przejrzysty i intuicyjny interfejs sieciowy, ale można go również używać w całości za pomocą wiersza poleceń. Jest napisany w Pythonie 3 i posiada licencję MIT.

Instancję SpiderFoot zhostowałem na VM linuxie Kali, skan trwał nieco ponad godzinę.

Spora ilość wyników związanych z cert.pl może być skutkiem obecności Alertu CERT



1. **Affiliate - Email Address**
    a. abuse@cloudflare.com
    b. noc@cloudflare.com
    c. rir@cloudflare.com
    d. abuse@nask.pl
    e. hostmaster@nask.pl
    f. registry@nask.pl

2. **BGP AS Membership**
    a. 13335 hovarokosak.com
    b. 8308 195.187.6.33
    c. 8308 195.187.0.0/18

3. **Blacklisted Affiliate Internet Name**

a. CleanBrowsing DNS - Security
b. Comodo Secure DNS
c. Quad9
d. Steven Black Hosts Blocklist

4. **Blacklisted IP on Same Subnet**
   a. VoIP Blacklist (VoIPBL) [195.187.0.0/18] hxxps://voipbl.org/check/?ip=195.187.0.0/18

5. **Blacklisted Internet Name**
   a. CleanBrowsing DNS - Security
   b. CloudFlare - Malware
   c. Comodo Secure DNS
   d. DNS for Family
   e. Quad9
   f. Steven Black Hosts Blocklist

6. **Co-hosted Site**
   a. cert.pl
   b. lista.cert.pl

7. **Co-hosted Site - Domain Name**
   a. cert.pl

8. **Country Name**
   a. Poland cert.pl
   b. United States hovarokosak.com

9. **Domain Name**
   a. hovarokosak.com

10. **Domain Name (Parent)**
    a. 554217.xyz 0-01x-merchandise.554217.xyz

11. **HTTP Headers**
    a. {"server": "nginx/1.14.2", "date": "Fri, 20 Oct 2023 19:45:46 GMT", "content-type": "text/html", "last-modified": "Thu, 19 Mar 2020 17:00:55 GMT", "transfer-encoding": "chunked", "etag": "W/\"5e73a547-37e8\"", "content-encoding": "gzip", "cache-control": "no-cache, max-age=10"}

12. **HTTP Status Code**
    a. 200 (będzie 200 na każdej subdomenie przez alert)

13. **IP Address**
    a. 195.187.6.33

14. **IP Address - Internal Network**
    a. 127.0.0.1

b. ::1

15. Internet Name

a. 0-01x-merchandise.554217.xyz
b. hovarokosak.com

16. Linked URL - External

a. http://0-01x-merchandise.554217.xyz/
b. https://cert.pl/ostrzezenia_phishing
c. https://gov.pl/koronawirus
d. https://incydent.cert.pl

17. Linked URL - Internal

a. hxxp://0-01x-merchandise.554217.xyz
b. hxxp://hovarokosak.com
c. hxxps://hovarokosak.com/ndjs4Hkd?utm_campaign=aua309orlspad1&utm_source=ORLEN&utm_content=aua309orlspad1&pixel=354431829978209&id_buyer=80&gi=629

18. Malicious Affiliate

a. CleanBrowsing DNS - Security
b. Comodo Secure DNS
c. Quad9
d. Steven Black Hosts Blacklist

19. Malicious IP on the Same Subnet

a. VoIP Blacklist (VoIPBL) [195.187.0.0/18] hxxps://voipbl.org/check/?ip=195.187.0.0/18

20. Netblock Membership

a. 195.187.0.0/18

21. Open TCP Port

a. 0-01x-merchandise.554217.xyz:443
b. 195.187.6.33:443
c. 195.187.6.33:80
d. hovarokosak.com:443

22. Physical Address

a. 101 Townsend Street, San Francisco, CA, 94107, US
b. ul. Kolska 12, 01-045, Warszawa, POLAND

23. Physical Coordinates

a. 37.780037,-122.391102

24. Physical Location

a. US
b. Warsaw, Mazovia, 14, Poland, PL

25. Raw DNS Records

a. 0-01x-merchandise.554217.xyz. 75390 IN NS localhost.
b. cocinabien.es. 86400 IN NS localhost.

26. Raw Data from RIRs/APIs

a. [{'issuer_ca_id': 183267, 'issuer_name': "C=US, O=Let's Encrypt, CN=R3", 'common_name': 'hovarokosak.com', 'name_value': 'hovarokosak.com', 'id': 10765191068, 'entry_timestamp': '2023-10-02T12:21:38.401', 'not_before': '2023-10-02T11:21:37', 'not_after': '2023-12-31T11:21:36', 'serial_number': '04aa97a697add65b8a9ebcc514afb4a5db4f'}, {'issuer_ca_id': 183267, 'issuer_name': "C=US, O=Let's Encrypt, CN=R3", 'common_name': 'hovarokosak.com', 'name_value': 'hovarokosak.com', 'id': 10570975709, 'entry_timestamp': '2023-10-02T12:21:37.911', 'not_before': '2023-10-02T11:21:37', 'not_after': '2023-12-31T11:21:36', 'serial_number': '04aa97a697add65b8a9ebcc514afb4a5db4f'}, {'issuer_ca_id': 180753, 'issuer_name': 'C=US, O=Google Trust Services LLC, CN=GTS CA 1P5', 'common_name': 'hovarokosak.com', 'name_value': '*.hovarokosak.com\nhovarokosak.com', 'id': 10742425790, 'entry_timestamp': '2023-10-02T12:18:55.212', 'not_before': '2023-10-02T11:18:54', 'not_after': '2023-12-31T11:18:53', 'serial_number': '00e02ca078644c4f3e0
b. [{'task': {'visibility': 'public', 'method': 'manual', 'domain': 'hovarokosak.com', 'apexDomain': 'hovarokosak.com', 'time': '2023-10-19T18:56:45.260Z', 'uuid': '0a0bffb3-fe23-46a0-a881-410d14280d59', 'url': 'https://hovarokosak.com/ndjs4Hkd?utm_campaign=aua309orlspad1&utm_source=ORLEN&utm_content=aua309orlspad1&pixel=354431829978209&id_buyer=80&gi=629'}, 'stats': {'uniqIPs': 1, 'uniqCountries': 1, 'dataLength': 2087, 'encodedDataLength': 1803, 'requests': 1}, 'page': {'country': 'US', 'server': 'cloudflare', 'ip': '172.67.150.246', 'mimeType': 'text/html', 'title': 'Document', 'url': 'https://hovarokosak.com/ndjs4Hkd?utm_campaign=aua309orlspad1&utm_source=ORLEN&utm_content=aua309orlspad1&pixel=354431829978209&id_buyer=80&gi=629', 'tlsValidDays': 89, 'tlsAgeDays': 17, 'tlsValidFrom': '2023-10-02T11:18:37.000Z', 'domain': 'hovarokosak.com', 'apexDomain': 'hovarokosak.com', 'asnname': 'CLOUDFLARENET, US', 'asn': 'AS13335', 'tlsIssuer': 'E1', 'status': '200'}, '_id': '0a0bffb3-fe23-46a0-a881-410d14280d59', '_sco
c. {'asn': 13335, 'name': 'CLOUDFLARENET', 'description_short': 'Cloudflare, Inc.', 'description_full': ['Cloudflare, Inc.'], 'country_code': 'US', 'website': 'https://www.cloudflare.com', 'email_contacts': ['abuse@cloudflare.com', 'noc@cloudflare.com', 'rir@cloudflare.com'], 'abuse_contacts': ['abuse@cloudflare.com'], 'looking_glass': None, 'traffic_estimation': None, 'traffic_ratio': 'Mostly Outbound', 'owner_address': ['101 Townsend Street', 'San Francisco', 'CA', '94107', 'US'], 'rir_allocation': {'rir_name': 'ARIN', 'country_code': 'US', 'date_allocated': '2010-07-14 00:00:00', 'allocation_status': 'assigned'}, 'iana_assignment': {'assignment_status':

'assigned', 'description': 'Assigned by ARIN', 'whois_server': 'whois.arin.net', 'date_assigned': None}, 'date_updated': '2023-10-06 07:44:26'}

27. SSL Certificate - Issued by

a. <Name(C=US,O=DigiCert Inc,OU=www.digicert.com,CN=RapidSSL TLS RSA CA G1)>

28. SSL Certificate - Issued to

a. <Name(CN=*.cert.pl)>

29. SSL Certificate - Raw Data

a.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:37:8c:09:8e:f8:b8:33:7b:fa:9c:ff:bd:3d:08:51:d7:02
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=US, O=Let's Encrypt, CN=E1
        Validity
            Not Before: Oct  2 11:18:37 2023 GMT
            Not After : Dec 31 11:18:36 2023 GMT
        Subject: CN=hovarokosak.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:a9:45:df:e7:3f:c4:c3:c0:8f:70:2b:a7:0e:2e:
                    46:80:42:5d:4c:08:a6:fd:f1:fa:51:15:d6:1f:69:
                    47:a2:ea:6e:c1:47:7a:f2:ca:d3:fc:54:88:13:84:
                    de:48:39:4a:3b:ac:42:6e:88:18:19:c1:9f:63:b4:
                    6e:d2:12:74:fe
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key U
```

b.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
```

04:aa:97:a6:97:ad:d6:5b:8a:9e:bc:c5:14:af:b4:a5:db:4f
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Let's Encrypt, CN=R3
Validity
Not Before: Oct 2 11:21:37 2023 GMT
Not After : Dec 31 11:21:36 2023 GMT
Subject: CN=hovarokosak.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:e6:c4:30:54:dc:4e:c2:ed:64:2e:ed:8c:31:68:
a0:f2:35:33:69:38:6d:a7:5f:11:c3:19:98:61:09:
54:fb:39:2f:1a:50:0e:f8:71:24:ce:16:b6:ee:83:
46:5c:97:b4:9a:4c:73:29:4a:5d:ea:02:7a:07:df:
c1:c1:26:95:ed:74:f5:09:b7:fb:26:db:b1:cf:88:
6e:d5:a2:09:7e:19:b3:f5:13:d6:58:2e:bf:24:68:
67:1b:b2:e9:be:98:90:71:d9:60:0d:38:a6:0e:f6:
27:be:41:da

c.

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
0c:18:e6:7b:e3:73:83:b8:4a:1f:99:d8:00:22:a1:18
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1
Validity
Not Before: Mar 29 00:00:00 2023 GMT
Not After : Mar 18 23:59:59 2024 GMT
Subject: CN=*.cert.pl
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:9f:16:13:85:1c:c6:68:bc:fa:01:4c:e0:88:9e:
e5:cc:c7:ce:b1:e7:23:5c:05:8e:67:d4:f8:d2:b5:
02:3b:cf:98:30:07:ba:df:91:7e:86:36:80:fd:20:
3f:c4:f9:f8:4b:0d:40:e6:50:5e:a4:49:21:d3:9f:
f7:b0:0a:b5:2c:ff:7b:23:34:75:1a:e5:d7:5f:03:
93:24:86:44:04:05:14:72:84:a2:06:2b:02:2b:21:
ac:91:b8:20:7b:fa:68:9d:38:85:f8:44:20:d0:ad:

d.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            e0:2c:a0:78:64:4c:4f:3e:0e:04:33:be:f9:eb:75:5d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
        Validity
            Not Before: Oct  2 11:18:54 2023 GMT
            Not After : Dec 31 11:18:53 2023 GMT
        Subject: CN=hovarokosak.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a6:ea:17:44:d7:ab:51:31:71:f9:72:c4:20:5a:
                    35:67:d9:77:85:90:d8:db:43:ad:ea:9a:d8:c8:59:
                    86:8f:da:39:a0:6a:ab:64:6b:4d:2f:b1:f7:9f:f6:
                    62:67:e0:3a:78:45:8b:1b:63:db:7e:7e:87:df:30:
                    f2:5d:ff:89:4b:68:f4:d7:41:bc:6c:52:eb:be:2b:
                    e6:59:37:3d:c8:75:64:b4:09:b8:0d:80:74:90:43:
                    78:4c:4b:04:b2:c1:f0:4f:a8:64:7b:f8:eb:ce:15:
```

30. SSL Certificate Host Mismatch

a. *.cert.pl, cert.pl -> hovarokosak.com
b. *.cert.pl, cert.pl -> 0-01x-merchandise.554217.xyz

31. Similar Domain

a. 554217.com
b. 554217.com.ye
c. 554217.cust.dev.thingdust.io
d. 554217.cust.disrec.thingdust.io
e. 554217.reservd.disrec.thingdust.io
f. hovarokosak.cust.dev.thingdust.io
g. hovarokosak.cust.disrec.thingdust.io
h. hovarokosak.net.ye
i. hovarokosak.reservd.disrec.thingdust.io

32. Web Content

a. text/html

33. Web Content Type

a. text/html

34. Web Server

a. cloudflare

    i. hovarokosak.com
b. nginx/1.14.2
    i. {"server": "nginx/1.14.2", "date": "Fri, 20 Oct 2023 19:45:46 GMT", "content-type": "text/html", "last-modified": "Thu, 19 Mar 2020 17:00:55 GMT", "transfer-encoding": "chunked", "etag": "W/\"5e73a547-37e8\"", "content-encoding": "gzip", "cache-control": "no-cache, max-age=10"}