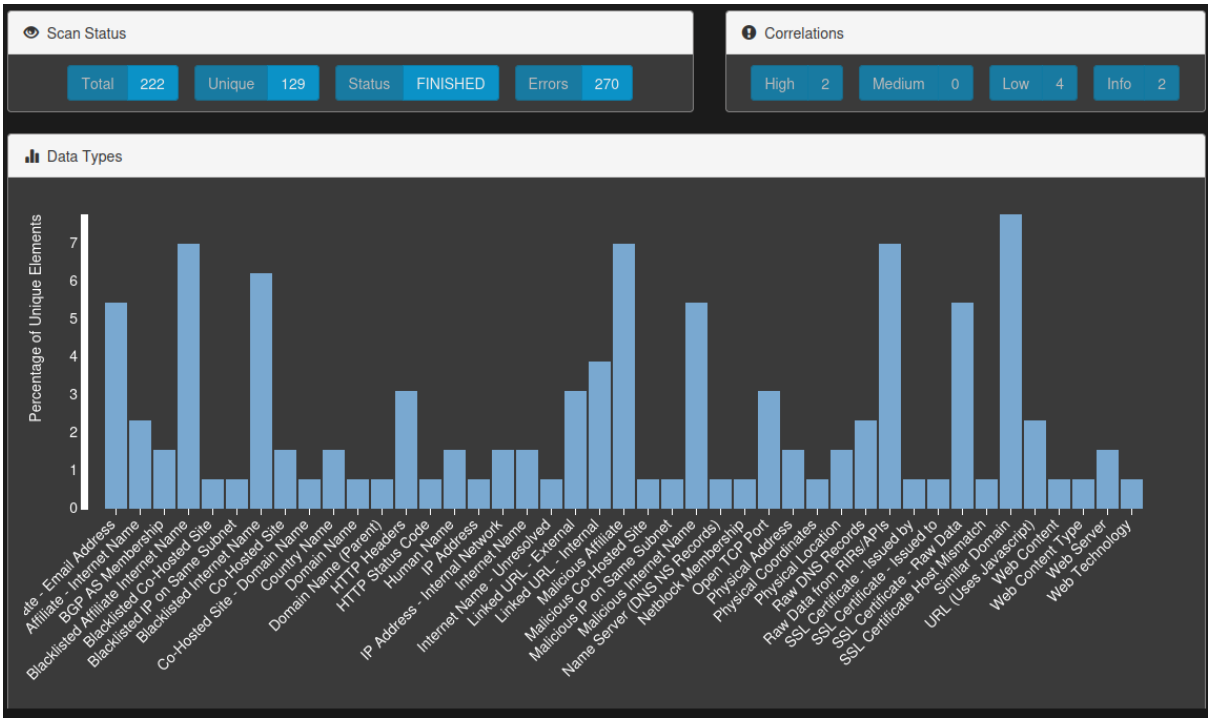
SpiderFoot analysis of cocinabien.es

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

Name	Target	Started	Finished	Status	Elements	Correlations
Cocina Bien 1	cocinabien.es	2023-10-20 20:33:21	2023-10-20 21:40:52	FINISHED	222	2 0 4 2



1. **Affiliate - Email Address**
    a. abuse@ionos.com
    b. noc@net.ionos.com
    c. ripe-role@net.ionos.com
    d. ripe-role@oneandone.net
    e. abuse@nask.pl
    f. hostmaster@nask.pl
    g. registry@nask.pl

2. **BGP AS Membership**
    a. 8308 195.187.6.33
    b. 8308 195.187.0.0/18
    c. 8560 cocinabien.es

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. Comodo Secure DNS
    c. DNS for Family
    d. OpenDNS - Phishing
    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. Spain cocinabien.es

9. **Domain Name**
    a. cocinabien.es

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 18:34:37 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. cocinabien.es

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://cocinabien.es
c. hxxp://cocinabien.es/cc.php

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. cocinabien.es:443

22. Physical Address

a. Hinterm Hauptbahnhof 5, 76137, Karlsruhe, GERMANY
b. ul. Kolska 12, 01-045, Warszawa, POLAND

23. Physical Coordinates

a. 48.9925206, 8.402208489812994

24. Physical Location

a. DE

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': 64138, 'issuer_name': 'C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1', 'common_name': '*.cocinabien.es', 'name_value': '*.cocinabien.es\ncocinabien.es', 'id': 8476313082, 'entry_timestamp': '2023-01-23T08:12:13.028', 'not_before': '2023-01-23T00:00:00', 'not_after': '2024-02-05T23:59:59', 'serial_number': '0e0111d0a078c82fe96747518b363d86'}, {'issuer_ca_id': 64138, 'issuer_name': 'C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1', 'common_name': '*.cocinabien.es', 'name_value': '*.cocinabien.es\ncocinabien.es', 'id': 6026558383, 'entry_timestamp': '2022-01-22T06:17:11.991', 'not_before': '2022-01-22T00:00:00', 'not_after': '2023-02-05T23:59:59', 'serial_number': '0ad1b300c2e9e500e974458384a3b735'}, {'issuer_ca_id': 64138, 'issuer_name': 'C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1', 'common_name': '*.cocinabien.es', 'name_value': '*.cocinabien.es\ncocinabien.es', 'id': 3966368479, 'e
b. [{'task': {'visibility': 'public', 'method': 'manual', 'domain': 'cocinabien.es', 'apexDomain': 'cocinabien.es', 'time': '2023-10-19T18:55:52.069Z', 'uuid': '378b12d3-eca8-414c-ab14-b80b6eb126e7', 'url': 'https://cocinabien.es/'}, 'stats': {'uniqIPs': 2, 'uniqCountries': 1, 'dataLength': 19361, 'encodedDataLength': 4073, 'requests': 2}, 'page': {'country': 'DE', 'server': 'Apache', 'ip': '2001:8d8:100f:f000::291', 'mimeType': 'text/html', 'url': 'https://cocinabien.es/', 'tlsValidDays': 378, 'tlsAgeDays': 269, 'tlsValidFrom': '2023-01-23T00:00:00.000Z', 'domain': 'cocinabien.es', 'apexDomain': 'cocinabien.es', 'asnname': 'IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE', 'asn': 'AS8560', 'tlsIssuer': 'Encryption Everywhere DV TLS CA - G1', 'status': '403'}, '_id': '378b12d3-eca8-414c-ab14-b80b6eb126e7', '_score': None, 'sort': [1697741752069, '378b12d3-eca8-414c-ab14-b80b6eb126e7'], 'result': 'https://urlscan.io/api/v1/
c. {'asn': 8560, 'name': 'IONOS-AS', 'description_short': 'This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE.', 'description_full': ['This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE.', '1&1 IONOS SE', 'Hinterm Hauptbahnhof 5', 'D-76137 Karlsruhe', 'Germany'], 'country_code': 'DE', 'website': 'http://www.ionos.com', 'email_contacts': ['abuse@ionos.com', 'ripe-role@oneandone.net', 'noc@net.ionos.com', 'ripe-role@net.ionos.com'], 'abuse_contacts': ['abuse@ionos.com'], 'looking_glass': None, 'traffic_estimation': '500-1000Gbps', 'traffic_ratio': 'Mostly Outbound',

'owner_address': ['Hinterm Hauptbahnhof 5', '76137', 'Karlsruhe', 'GERMANY'], 'rir_allocation': {'rir_name': 'RIPE', 'country_code': 'DE', 'date_allocated': '1997-11-26 00:00:00', 'allocation_status': 'allocated'}, 'iana_assignment': {'assignment_status': 'assigned', 'description': 'Assigned by RIPE NCC', '

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:
05:f9:f8:1b:fc:8b:1b:c8:60:b2:28:06:65:2f:1b:be
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
Validity
Not Before: Jan 19 00:00:00 2019 GMT
Not After : Jan 19 12:00:00 2020 GMT
Subject: CN=*.cocinabien.es
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:88:7b:1b:43:f8:e4:25:f2:c5:07:c3:fd:a2:ec:
25:3f:89:75:bb:8a:11:55:a7:29:b7:fc:e4:79:f0:
54:09:3f:15:b9:7a:a3:63:c8:73:ca:88:b6:7f:45:
64:47:26:05:bf:c5:f3:bb:71:7a:6f:e0:a7:78:74:
d7:5a:9f:c1:05:76:dc:51:85:98:58:48:3d:24:02:
c7:2c:5b:df:49:1e:a5:d6:55:2b:bf:b9:a1:bb:04:
c7:39:d9:4f:ed:c3:a5:a7:b5:5f

b.

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
06:80:80:91:2b:b6:ae:a7:71:69:6a:27:28:33:24:cc
Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
Validity
Not Before: Jan 22 00:00:00 2021 GMT
Not After : Feb 4 23:59:59 2022 GMT
Subject: CN=*.cocinabien.es
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:8b:7d:31:e0:be:4e:72:fd:b3:5b:aa:46:7f:fe:
d1:ab:49:35:20:84:04:24:1b:e2:db:9a:77:73:f7:
83:3a:92:ed:10:8f:46:58:7a:6a:86:fe:62:35:cc:
7d:cf:26:19:2e:b9:0d:2d:2d:85:0a:d8:80:c0:83:
73:1d:98:0b:48:e1:79:8c:6b:aa:82:36:9f:c0:72:
94:70:cf:20:8f:29:b1:a7:83:09:17:68:f4:82:f0:
82:0a:f7:ca:f0:b4:49:a8:f4:34

c.

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
08:e2:d3:74:8d:ea:8e:23:fe:1b:62:84:f3:c2:60:19
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
Validity
Not Before: Jan 7 00:00:00 2020 GMT
Not After : Feb 5 12:00:00 2021 GMT
Subject: CN=*.cocinabien.es
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:97:57:0b:91:6a:19:60:72:91:0c:64:f7:b0:53:
33:9e:1e:a2:a5:cd:de:84:5c:a2:17:69:d5:98:97:
c8:38:72:fb:95:c6:ff:45:11:f9:16:5e:58:4d:09:
4a:af:2a:7a:d8:ec:28:cf:00:8d:0b:03:b4:54:08:
3c:6d:32:07:8e:b5:60:01:89:54:7e:56:7d:a7:03:
f7:98:bb:b7:68:70:7e:6e:d0:a8:17:fa:c8:2e:31:
c6:1f:94:7c:c4:f5:e6:d3:62:45

d.

Certificate:
Data:
Version: 3 (0x2)

Serial Number:
0a:d1:b3:00:c2:e9:e5:00:e9:74:45:83:84:a3:b7:35
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV TLS CA - G1
Validity
Not Before: Jan 22 00:00:00 2022 GMT
Not After : Feb 5 23:59:59 2023 GMT
Subject: CN=*.cocinabien.es
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:88:c2:8d:4c:14:90:9c:a2:00:58:fc:9a:f5:83:
03:39:65:20:d6:f5:cb:de:82:84:37:96:d9:45:ff:
83:f2:24:e2:67:ea:35:00:7d:2d:15:e7:19:81:34:
7c:7f:99:91:6e:78:15:ef:61:d3:d0:f7:eb:6e:f7:
89:6d:3c:ac:b1:b2:b3:39:70:e7:ef:fb:bc:50:c6:
16:8c:82:c8:c6:df:a8:f4:3a:2e:f5:f6:22:2e:d0:
2b:53:59:5e:9b:0d:96:59:ae:f9

e.
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:

f.
Certificate:

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:e5:fa:f3:5f:0e:50:2d:00:a6:d3:45:af:1b:bb:75
        Signature Algorithm: sha256WithRSAEncryption
         Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV
TLS CA - G2
        Validity
            Not Before: Feb  2 00:00:00 2018 GMT
            Not After : Feb  2 12:00:00 2019 GMT
        Subject: CN=www.cocinabien.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c2:9e:e2:cb:b5:a1:50:a6:d6:60:28:39:8a:eb:
                    f5:53:3c:39:3a:8e:ec:ba:07:45:4d:01:51:a0:5a:
                    0c:2b:83:52:41:63:21:c7:31:3f:a1:6a:c5:3b:8b:
                    71:38:da:e8:23:e1:3d:ef:7d:cf:de:0f:6f:4e:10:
                    cd:6a:05:4e:eb:3c:33:41:da:ed:19:53:52:e2:f6:
                    69:f5:21:a3:e4:88:eb:4f:fc:e1:c5:6f:a0:75:87:
                    b4:a6:28:3c:3e:5e:35:c5:1f:

                 g.
            Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0e:01:11:d0:a0:78:c8:2f:e9:67:47:51:8b:36:3d:86
        Signature Algorithm: sha256WithRSAEncryption
         Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=Encryption Everywhere DV
TLS CA - G1
        Validity
            Not Before: Jan 23 00:00:00 2023 GMT
            Not After : Feb  5 23:59:59 2024 GMT
        Subject: CN=*.cocinabien.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:08:66:b2:9c:f4:70:06:26:90:05:2a:61:23:
                    28:f3:bb:c0:af:6f:db:14:9d:8b:94:af:83:a7:93:
                    9d:3f:f6:7f:12:20:04:60:fd:12:aa:4b:10:de:7b:
                    d9:aa:f0:3e:a7:5d:30:ec:0b:e8:63:b2:bb:7a:8a:
                    c4:33:d3:d0:2e:e3:38:ea:88:dd:d7:6d:05:2c:f7:
                    38:8f:4a:23:ae:2a:0d:89:f1:8b:69:f6:10:cc:ad:
                    60:45:c4:d0:fb:0a:e2:75:14:35
```

30. SSL Certificate Host Mismatch

a. *.cert.pl, cert.pl -> cocinabien.es
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. cocinabien.com
g. cocinabien.cust.dev.thingdust.io
h. cocinabien.cust.disrec.thingdust.io
i. cocinabien.online
j. cocinabien.reservd.disrec.thingdust.io

32. Web Content

a. text/html

33. Web Content Type

a. Apache
    i. cocinabien.es
b. nginx/1.14.2
    i. {"server": "nginx/1.14.2", "date": "Fri, 20 Oct 2023 18:34:37 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"}

34. Web Server

a. PHP
    i. {"server": "nginx/1.14.2", "date": "Fri, 20 Oct 2023 18:37:39 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"}