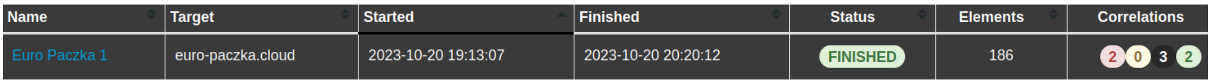
SpiderFoot analysis of euro-paczka.cloud

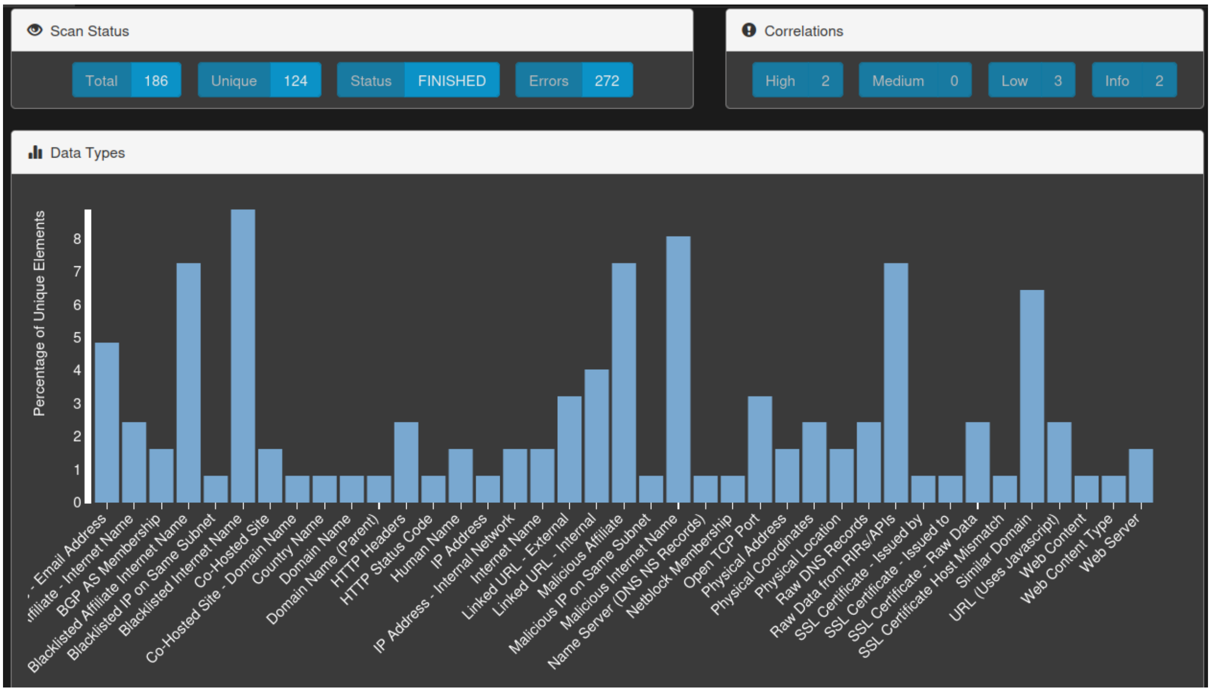
SpiderFoot to narzędzie do automatyzacji wywiadu typu open source (OSINT). Integruje się z niemal każdym dostępnym źródłem danych i wykorzystuje szereg metod analizy danych, dzięki czemu nawigacja po nich jest łatwa. SpiderFoot ma wbudowany serwer sieciowy zapewniający przejrzysty i intuicyjny interfejs 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
Euro Paczka 1	euro-paczka.cloud	2023-10-20 19:13:07	2023-10-20 20:20:12	FINISHED	186	2 0 3 2



Scan Status

Total 186 | Unique 124 | Status FINISHED | Errors 272

Correlations

High 2 | Medium 0 | Low 3 | Info 2

Data Types

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 euro-paczka.cloud
    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 Blacklist

4. **Blacklisted IP on Same Subnet**
   a. VoIP Blacklist (VoIPBL) [195.187.0.0/18]

5. **Blacklisted Internet Name**
   a. CleanBrowsing DNS - Security
   b. Comodo Secure DNS
   c. DNS for Family
   d. OpenDNS
   e. Quad9
   f. SURBL
   g. Steven Black Hosts Blacklist

6. **Co-hosted Site**
   a. Cert.pl source: sfp_sslcert
   b. lista.cert.pl source: sfp_hackertarget

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

8. **Country Name**
   a. Poland

9. **Domain Name**
   a. euro-paczka.cloud

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

11. **HTTP Headers**
    a. "server": "nginx/1.14.2",
    b. "date": "Fri, 20 Oct 2023 17:14:24 GMT",
    c. "content-type": "text/html",
    d. "last-modified": "Thu, 19 Mar 2020 17:00:55 GMT",
    e. "transfer-encoding": "chunked",
    f. "etag": "W/\"5e73a547-37e8\"",
    g. "content-encoding": "gzip",
    h. "cache-control": "no-cache,
    i. max-age=10"

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

13. **IP Address**

a. 195.187.6.33 source: sfp_dnsresolve

14. IP Address - Internal Network

a. 127.0.0.1
b. ::1

15. Internet Name

a. 0-01x-merchandise.554217.xyz
b. euro-paczka.cloud

16. Linked URL - External

a. hxxp://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. hxxps://euro-paczka.cloud/921747
c. hxxps://euro-paczka.cloud/RNhd129BmmrUGOmc4uG/1eirNo

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. euro-paczka.cloud: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. 37.78,-122.39
b. 52.25, 20.98

24. Physical Location

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

25. Raw DNS Records

a. 0-01x-merchandise.554217.xyz. 80179 IN NS localhost.
b. euro-paczka.cloud. 83908 IN NS localhost.

26. Raw Data from RIRs/APIs

a. [{'issuer_ca_id': 105484, 'issuer_name': 'C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA', 'common_name': 'euro-paczka.cloud', 'name_value': '*.euro-paczka.cloud\neuro-paczka.cloud', 'id': 10792711268, 'entry_timestamp': '2023-10-15T15:19:14.914', 'not_before': '2023-10-15T00:00:00', 'not_after': '2024-10-14T23:59:59', 'serial_number': '00bcd7267f5a3f1c51ceefc2a047d7eeec'}, {'issuer_ca_id': 105484, 'issuer_name': 'C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA', 'common_name': 'euro-paczka.cloud', 'name_value': '*.euro-paczka.cloud\neuro-paczka.cloud', 'id': 10792710252, 'entry_timestamp': '2023-10-15T15:19:13.94', 'not_before': '2023-10-15T00:00:00', 'not_after': '2024-10-14T23:59:59', 'serial_number': '00bcd7267f5a3f1c51ceefc2a047d7eeec'}, {'issuer_ca_id': 180753, 'issuer_name': 'C=US, O=Google Trust Services LLC, CN=GTS CA 1P5', 'common_name': 'euro-paczka.cloud', 'name_value': '*.eur

b. [{'task': {'visibility': 'public', 'method': 'api', 'domain': '0-01x-merchandise.554217.xyz', 'apexDomain': '554217.xyz', 'time': '2022-08-11T10:45:12.815Z', 'uuid': 'd72100cb-11b2-49bf-b709-e9d15cb9e046', 'url': 'http://0-01x-merchandise.554217.xyz'}, 'stats': {'uniqIPs': 2, 'uniqCountries': 1, 'dataLength': 25781, 'encodedDataLength': 11313, 'requests': 4}, 'page': {'country': 'US', 'server': 'cloudflare', 'redirected': 'same-domain', 'ip': '2a06:98c1:3120::3', 'domain': '0-01x-merchandise.554217.xyz', 'apexDomain': '554217.xyz', 'mimeType': 'text/html', 'asnname': 'CLOUDFLARENET, US', 'title': 'Access denied', 'asn': 'AS13335', 'url': 'http://0-01x-merchandise.554217.xyz/', 'status': '403'}, '_id': 'd72100cb-11b2-49bf-b709-e9d15cb9e046', '_score': None, 'sort': [1660214712815, 'd72100cb-11b2-49bf-b709-e9d15cb9e046'], 'result': 'https://urlscan.io/api/v1/result/d72100cb-11b2-49bf-b709-e9d15cb9e046/', 'screenshot': 'https://urlscan.io/screenshots/d72100cb-11b2-49bf-b709-e9d15cb9e046.png' }, {'task': {'visibil

c. [{'task': {'visibility': 'public', 'method': 'manual', 'domain': 'euro-paczka.cloud', 'apexDomain': 'euro-paczka.cloud', 'time': '2023-10-15T19:52:38.098Z', 'uuid': '302fbd51-86bf-4687-849d-c58451d23b0d', 'url': 'https://euro-paczka.cloud/RNhd129BmmrUGOmc4uG/1eirNo'}, 'stats': {'uniqIPs': 1, 'uniqCountries': 1, 'dataLength': 757966, 'encodedDataLength': 661290, 'requests': 11}, 'page': {'country': 'US', 'server': 'cloudflare', 'ip':

'2a06:98c1:3121::3', 'mimeType': 'text/html', 'title': 'PayU', 'url': 'https://euro-paczka.cloud/RNhd129BmmrUGOmc4uG/1eirNo', 'tlsValidDays': 89, 'tlsAgeDays': 0, 'tlsValidFrom': '2023-10-15T13:54:49.000Z', 'domain': 'euro-paczka.cloud', 'apexDomain': 'euro-paczka.cloud', 'asnname': 'CLOUDFLARENET, US', 'asn': 'AS13335', 'tlsIssuer': 'GTS CA 1P5', 'status': '200'}, '_id': '302fbd51-86bf-4687-849d-c58451d23b0d', '_score': None, 'sort': [1697399558098, '302fbd51-86bf-4687-849d-c58451d23b0d'], 'result': 'https://urlscan.io/api/v1/result/302fbd51-86bf-4687-849d-c58451d23b0d/', 'screen

d. {'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:
            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:
```

b.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            99:14:e9:12:d1:3d:95:f2:0e:cb:ef:97:37:b1:d1:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
        Validity
            Not Before: Oct 15 13:54:49 2023 GMT
            Not After : Jan 13 13:54:48 2024 GMT
        Subject: CN=euro-paczka.cloud
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:92:7f:dc:9a:64:60:49:88:7d:9a:a3:6b:7d:ed:
                    31:3f:01:40:bd:dc:b9:fc:5f:ab:81:08:0a:f3:fe:
                    7e:b0:b4:a8:aa:82:e4:32:dc:90:f5:55:28:70:63:
                    ec:df:45:84:47:43:77:82:5d:0b:37:70:87:d9:d6:
                    a0:e1:e5:44:e3:6d:b7:2c:9b:40:34:ab:64:7c:5c:
                    29:c0:4c:e2:a9:04:1c:fa:7a:d6:06:a4:a9:b3:64:
                    8d:21:c6:0f:ba:8e:fd:b0:88:73:f4:08:70:a5:6b:
```

c.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:d7:26:7f:5a:3f:1c:51:ce:ef:c2:a0:47:d7:ee:ec
        Signature Algorithm: ecdsa-with-SHA256
          Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited,
CN=Sectigo ECC Domain Validation Secure Server CA
        Validity
            Not Before: Oct 15 00:00:00 2023 GMT
            Not After : Oct 14 23:59:59 2024 GMT
        Subject: CN=euro-paczka.cloud
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:fe:c2:db:19:1a:46:bf:a2:1e:06:2a:4a:4e:51:
```

```
            20:70:53:89:e0:f8:e0:ef:f3:4c:33:ff:9a:8b:37:
            ef:85:ff:8e:fd:d2:ca:a7:15:e3:b1:f5:c5:8e:99:
            39:18:ef:cd:7f:e1:c6:44:42:1e:65:6d:50:6f:c1:
            06:1d:aa:a3:29
          ASN1 OID: prime256v1
          NIST CURVE: P-256
      X509v3 extensions:
        X509v3 Authority K
```

30. SSL Certificate Host Mismatch

a. *.cert.pl -> euro-paczka.cloud
b. *.cert.pl -> 0-01x-merchandise.554217.xyz

31. Similar Domain

a. euro-paczka.cloud
   - i. euro-paczka.cust.dev.thingdust.io
   - ii. euro-paczka.cust.disrec.thingdust.io
   - iii. euro-paczka.edu.ye
   - iv. euro-paczka.reservd.disrec.thingdust.io

b. 0-01x-merchandise.554217.xyz
   - i. 554217.com
   - ii. 554217.cust.dev.thingdust.io
   - iii. 554217.cust.disrec.thingdust.io
   - iv. 554217.reservd.disrec.thingdust.io

32. Web Content

a. Uwaga! Zagrożenie!

33. Web Content Type

a. text/html

34. Web Server

a. cloudflare

b. nginx/1.14.2

i. {"server": "nginx/1.14.2", "date": "Fri, 20 Oct 2023 17:14:24 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"}