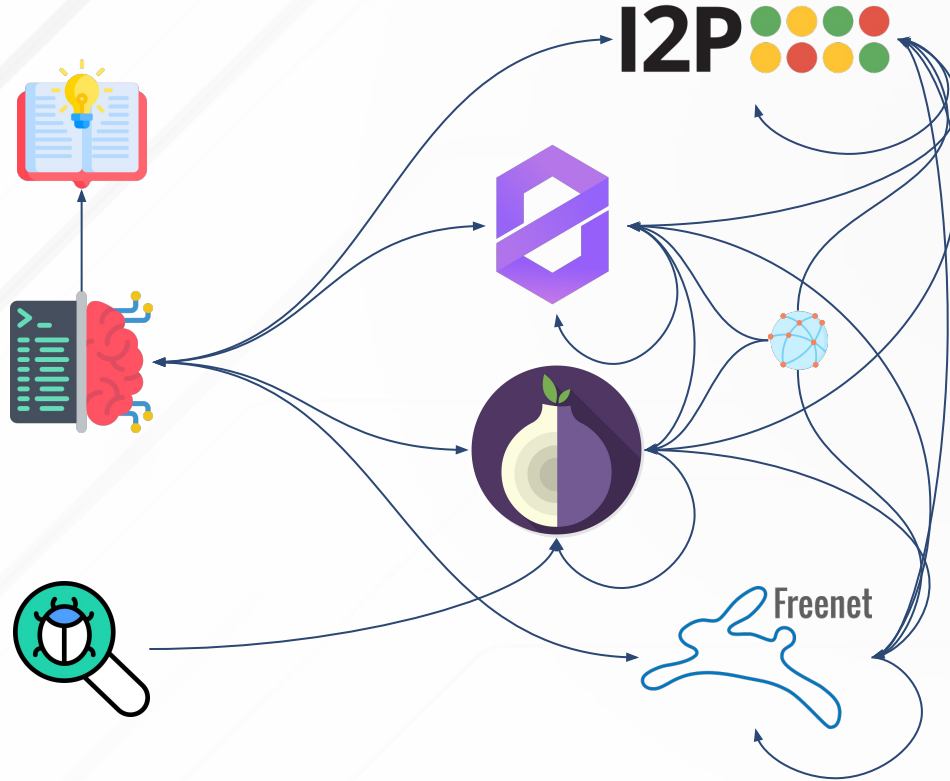




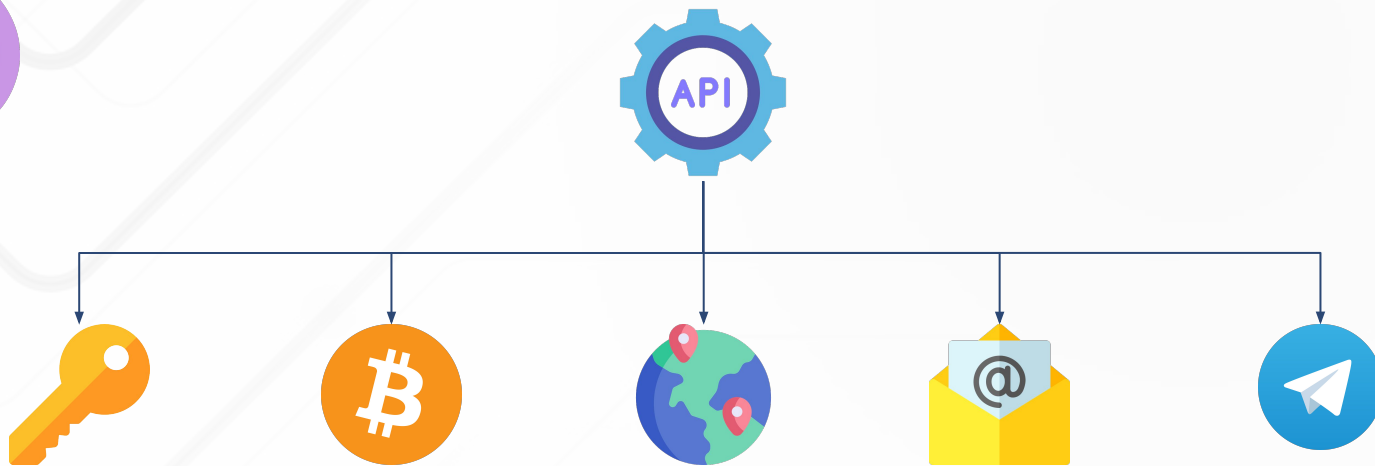
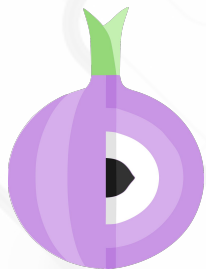
Byron Labs

A Cybersecurity Research Startup

Vysion



Product - Vysion



Data Breach

```
curl --location --request GET 'api.vysion.ai/api/v1/search/Volvo data  
breach?exact=true' \  
--header 'Accept: application/json' \  
--header "x-api-key:$API_KEY" | jq
```



Data breaches and leaks

```

{
  "data": {
    "total": 396,
    "hits": [
      {
        "page": {
          "id": "62b65db465d203864233ef8c",
          "url": {
            "protocol": "http",
            "domain": "i3osckqha5os4bpojodgvmv4vgqqycwbjy2qsv4wf4nxtjf53wiizid.onion",
            "port": 80,
            "path": "/index1c8b.php",
            "signature": "79b5a059ef4507df5798f4641134adc6",
            "network": "tor"
          },
          "parent": "d9143c1bd12ef881daf3fd99cbc1b090",
          "title": "Dark Leak Market",
          "language": "en",
          "html": "pid=58\><b>Volvo</b> <b>data</b> <b>breach</b></a></li>\n",
          "sha1sum": "9eb68b18c5a6be46b024cead95af31d98e93af31",
          "ssdeep": "96:nE3jgwC19GLoQhSYiHYeUjP1M17b+/CSokhLHMkM:ojw+neURRjtM",
        }
      ]
    }
  }
}

```

Dark Leak Market

Volvo data breach

File Name: Volvodatabreach.rar
File Size: 56GB
File Type: rar
Price: \$300

Pay 0.007941 BTC



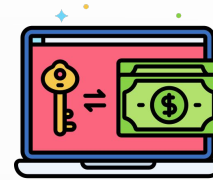
bc1qmdft9hvf8wzph060pwwjfu56hcstspxxg44hvl



Waiting for at least 3 Confirmations.

Alert - The Above Mentioned Address is for Bitcoin Only. And valid for single transaction. The payment address will change wh

Ransomware



```
curl --location --request GET 'api.vysion.ai/api/v1/search/Alliance  
Steel?exact=true' \  
--header 'Accept: application/json' \  
--header "x-api-key:$API_KEY" | jq
```

Product - Vysion

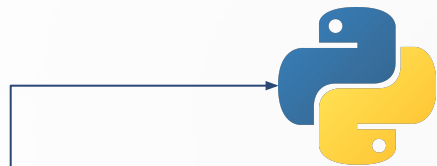
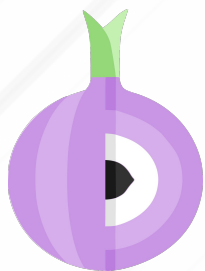
```
"data": {
  "total": 3,
  "hits": [
    {
      "page": {
        "id": "62a577c3cc3f18d96d5f8f91",
        "url": {
          "protocol": "http",
          "domain": "continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion",
          "port": 80,
          "path": "/page/1",
          "signature": "b98ac5263e3d01bc250f415793926f7a",
          "network": "tor"
        },
        "parent": "6ea95f6de8a1f571deab78e41eb5ca2f",
        "title": "CONTI.News",
        "language": "en",
        "html": "published\\:100,\\links\\:\\\"https:\\/\\/www.allianceokc.com\\nhttps:\\/\\/\\",
        "sha1sum": "dd214eef57ffe10ee18220ae56f0121591b56b05",
        "ssdeep": "192:4jG6T4G0leT/GDleTWgUSBXQUgzF3q3Fo1abCdeT9rXXFvE8IM:4y44r/b3FealBkeTFXXFvE8IM",
        "date": "2022-06-12T05:21:07.408403",
```



Banks

```
curl --location --request GET 'api.vysion.ai/api/v1/search/santander
banco?exact=true' \
--header 'Accept: application/json' \
--header "x-api-key:$API_KEY" | jq
```


Product - Vysion



Banks

```
from vysion import client

c = client.Client(api_key=API_KEY)
result = c.search("contileaks")

for hit in result.hits:
    print(hit.page.title)
```

Enrichment Results



Below you can see the attributes and objects that are to be created from the results of the enrichment module.

Event ID	1275
Event UUID	540a3112-0115-460a-a73a-26c4542c571c
Event creator org	Testing org
# of resolved Attributes	51 (10 objects)

Import	Category	Type	Value	Tags	IDS	Disable Correlation	Comment	Distribution
<div style="background-color: #004a99; color: white; padding: 5px;"> ✓ Name: vysion-page 🔗 References: 0 </div>								
<input checked="" type="checkbox"/>	Other	id text	62a2de29f4b28eceb98eb71f		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Network activity	url url	http://7fzrei37r2lkjnyqvra5br4n6dk4a5gfyggfp7ydsugmzkk67apid.onion:80/bank-accounts.html		<input checked="" type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Other	network text	tor		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<div style="background-color: #004a99; color: white; padding: 5px;"> ✓ Name: vysion-page 🔗 References: 0 </div>								
<input checked="" type="checkbox"/>	Other	id text	615483c0b8968e7d85c9b96e		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Network activity	url url	http://23uud7qmaq2nu7kvwvwyzqnfurqjrc26n45afhpwf5qf26drg2vid.onion:80/bank_accounts		<input checked="" type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Other	network text	tor		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<div style="background-color: #004a99; color: white; padding: 5px;"> ✓ Name: vysion-page 🔗 References: 0 </div>								
<input checked="" type="checkbox"/>	Other	id text	616a38e9a72a8244a7a8b3c6		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Network activity	url url	http://xrlvebokxn22g6x5gmq3cp7rsv3ar5zpirzyqlc4kshwfpnpl2zucdqd.onion:80/node/147712/index.html		<input checked="" type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Other	network text	tor		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<div style="background-color: #004a99; color: white; padding: 5px;"> ✓ Name: vysion-page 🔗 References: 0 </div>								
<input checked="" type="checkbox"/>	Other	id text	619ae8f236275b24ea61dfc		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Network activity	url url	http://xrlvebokxn22g6x5gmq3cp7rsv3ar5zpirzyqlc4kshwfpnpl2zucdqd.onion:80/node/147713/index.html		<input checked="" type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event
<input checked="" type="checkbox"/>	Other	network text	tor		<input type="checkbox"/>	<input type="checkbox"/>	banco santander: Enriched via th	Inherit event

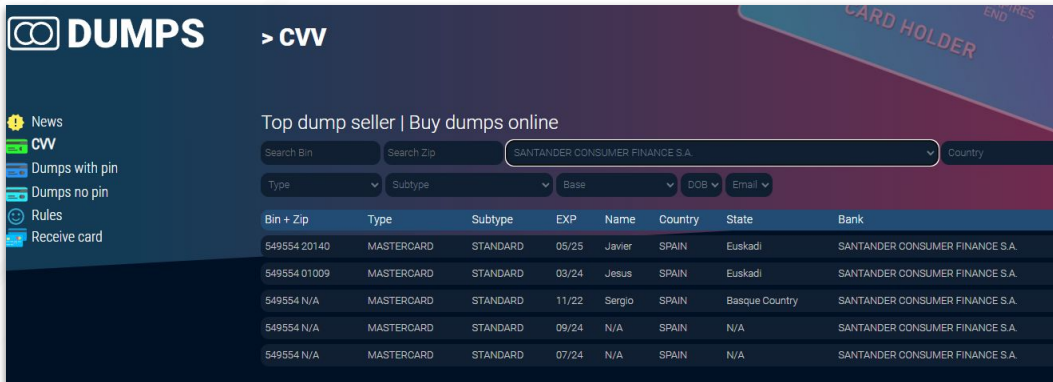
Credit cards



```
"page": {
  "id": "626b967a08ec5e2da6e40ba1",
  "url": {
    "protocol": "http",
    "domain": "2tdzk5dtffq67hn7k2fzpz3gpr7ibcowqa2g2pejff6tlbh6bxcze2lhqd.onion",
    "port": 80,
    "path": "/cvv/index.html",
    "signature": "d94232cd317f8ca81abdecc590376841",
    "network": "tor"
  },
  "parent": "777f9c81a846d7ef8bf48fb049bb4e93",
  "title": "Maximum quality dump shop | Buy credit cards\r\n",
  "language": "en",
  "html": "DE BANCA MULTIPLE GRUPO FINANCIERO <b>SANTANDER</b>\"><b>BANCO</b>",
  "sha1sum": "f33de5b556ccc0e0cf44fecfebabc577ee3e0ae9",
  "ssdeep": "3072:DxS7mzcbZ07PfePa5g5q98AXjMt60fVcRmq0WL80:8ucbZ07PIAb0fVZWL80",
  "date": "2022-06-19T06:39:59.371314",
  "chunk": true
},
"parent": "777f9c81a846d7ef8bf48fb049bb4e93",
```

Cached Version

```
cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.0/umd/popper.min.js"></script>\r\n <script src=\"../
maxcdn.bootstrapcdn.com/bootstrap/4.5.2/js/bootstrap.min.js"></script>\t\r\n<!-- End modal payment
-->\r\n\r\n<div class=\"tlgbot\"><a href=\"https://telegram.im/riodwf\"><img src=\"../assets/img/
telegram_logo.svg\"></a></div>\r\n\t<script src=\"../assets/js/bootstrap.min.js\"></
script>\r\n\t<script src=\"../assets/js/script.js\"></script>\r\n\t<script src=\"../assets/js/cart.
js\"></script>\r\n\r\n</body>\r\n\r\n<!-- Mirrored from carderescrow.com/cvv/ by HTTrack Website
Copier/3.x [XR&CO'2014], Sun, 03 Apr 2022 12:47:03 GMT -->\r\n</html>\r\n\r\n\",
"sha1sum": "f33de5b556cccc0e0cf44fecfebabc577ee3e0ae9",
"ssdeep": "3072:DxS7mzcbZ07PfEPa5g5q98AXjMt60fVcRmq@WL80:8ucbZ07PIAb0fVZWL80",
"date": "2022-06-19T05:39:59.371314",
"chunk": false
```



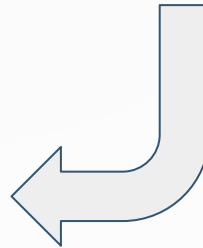
DUMPS > cvw

Top dump seller | Buy dumps online

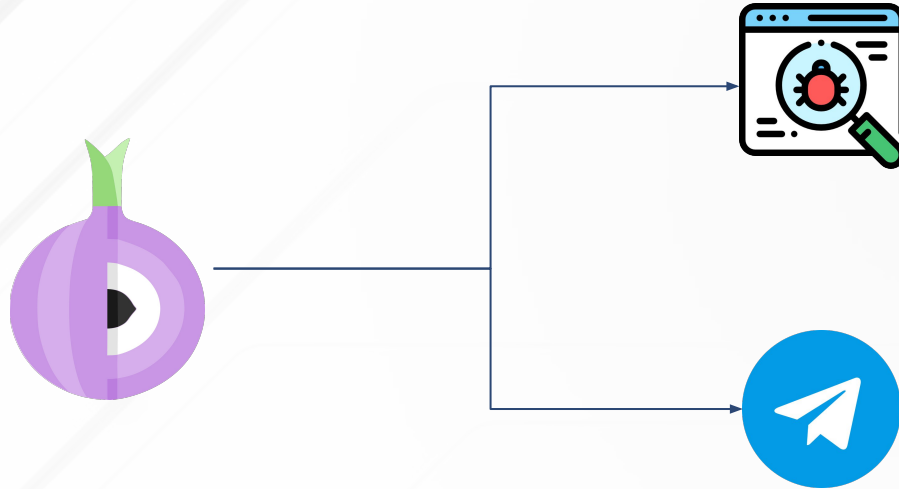
Search Bin: Search Zip: SANTANDER CONSUMER FINANCE S.A. Country: [dropdown]

Type: [dropdown] Subtype: [dropdown] Base: [dropdown] DCB: [dropdown] Email: [dropdown]

Bin + Zip	Type	Subtype	EXP	Name	Country	State	Bank
549554 20140	MASTERCARD	STANDARD	05/25	Javier	SPAIN	Euskadi	SANTANDER CONSUMER FINANCE S.A.
549554 01009	MASTERCARD	STANDARD	03/24	Jesus	SPAIN	Euskadi	SANTANDER CONSUMER FINANCE S.A.
549554 N/A	MASTERCARD	STANDARD	11/22	Sergio	SPAIN	Basque Country	SANTANDER CONSUMER FINANCE S.A.
549554 N/A	MASTERCARD	STANDARD	09/24	N/A	SPAIN	N/A	SANTANDER CONSUMER FINANCE S.A.
549554 N/A	MASTERCARD	STANDARD	07/24	N/A	SPAIN	N/A	SANTANDER CONSUMER FINANCE S.A.



Information feeds



Ransomware Feed

```
curl --location --request GET  
'api.vysion.ai/api/v1/feed/ransomware?batch=2022-06-19' \  
--header 'Accept: application/json' \  
--header "x-api-key:$API_KEY" | jq
```

31 groups monitored



Ransomware Feed

```
1  {
2  "data": {
3    "total": 5,
4    "hits": [
5      {
6        "id": "690026f1a0b539c23bd51d9e10752fd0fa8ccb399371578b9e73bf068cbc1f7d",
7        "company": "PT Astra Honda Motor",
8        "company_link": "http://www.astra-honda.com/",
9        "link": "http://ecdmr42a34qovoph557zotkfvth4fsz56twwvgiylstjup4r5bpc4oad.onion/JhykowedsgX/UdfGe4kmvb81sp/",
10       "group": "Vice Society",
11       "date": "2022-06-27T14:17:32",
12       "info": " Indonesia PT Astra Honda Motor is a motorcycle manufacturer based in Jakarta, Indonesia. It is a
13         joint venture between Honda and Astra International. "
14     },
15     {
16       "id": "b2df58acf21cc6abb423857d5c19bc265797be6c4aa1075d079e9dfc9eff8a36",
17       "company": "Pilton Community College",
18       "company_link": "http://www.piltoncollege.org.uk/",
19       "link": "http://ecdmr42a34qovoph557zotkfvth4fsz56twwvgiylstjup4r5bpc4oad.onion/JhykowedsgX/dsw64P0Gk1t8Xx/",
20       "group": "Vice Society",
21       "date": "2022-06-27T14:17:32",
22       "info": " United Kingdom Pilton Community College is a coeducational secondary school with academy status,
23         located in the Pilton area of Barnstaple in the English county of Devon. "
```

Questions?

carlos.cilleruelo@byronlabs.io | javier.junquera@byronlabs.io

`/in/carlos-cilleruelo/` | `/in/junquera`