raven-med.local   https://smartbear.com   IT   raven-m

image.png
image not found or type unknown

shodan

18.154.227.109

DNS   DNS

image.png
image not found or type unknown

```
└─# nslookup smartbear.com
Server:         8.8.8.8
Address:        8.8.8.8#53


Non-authoritative answer:
Name:   smartbear.com
Address: 65.8.20.55
Name:   smartbear.com
Address: 65.8.20.33
Name:   smartbear.com
Address: 65.8.20.8
Name:   smartbear.com
Address: 65.8.20.128
```

DNS


```
PS C:\Users\ntsystem> nslookup smartbear.com
Server:   cdns02.comcast.net
Address:   2001:558:feed::2


Non-authoritative answer:
Name:       smartbear.com
Addresses:  13.225.223.61
            13.225.223.46
            13.225.223.4
            13.225.223.25
```

Comcast

Route 53

Whois

```
┌──(root㉿kali)-[/opt/OneForAll]
└─# whois smartbear.com
   Domain Name: SMARTBEAR.COM
   Registry Domain ID: 100038507_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2022-09-04T07:44:21Z
   Creation Date: 2003-07-03T18:16:08Z
   Registry Expiry Date: 2025-07-03T18:16:08Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1416.AWSDNS-49.ORG
   Name Server: NS-1701.AWSDNS-20.CO.UK
   Name Server: NS-431.AWSDNS-53.COM
   Name Server: NS-917.AWSDNS-50.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-01-06T23:05:28Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
```

```
└─# whois smartbear.com

   Domain Name: SMARTBEAR.COM

   Registry Domain ID: 100038507_DOMAIN_COM-VRSN

   Registrar WHOIS Server: whois.godaddy.com

   Registrar URL: http://www.godaddy.com

   Updated Date: 2022-09-04T07:44:21Z

   Creation Date: 2003-07-03T18:16:08Z

   Registry Expiry Date: 2025-07-03T18:16:08Z
```

```
    Registrar: GoDaddy.com, LLC

    Registrar IANA ID: 146

    Registrar Abuse Contact Email: abuse@godaddy.com

    Registrar Abuse Contact Phone: 480-624-2505

    Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited

    Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited

    Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

    Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

    Name Server: NS-1416.AWSDNS-49.ORG

    Name Server: NS-1701.AWSDNS-20.CO.UK

    Name Server: NS-431.AWSDNS-53.COM

    Name Server: NS-917.AWSDNS-50.NET

    DNSSEC: unsigned

    URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-01-06T23:05:28Z <<<


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


NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.


TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
```

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: SMARTBEAR.COM
Registry Domain ID: 100038507_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2016-07-04T05:51:05Z
Creation Date: 2003-07-03T13:16:08Z
Registrar Registration Expiration Date: 2025-07-03T13:16:08Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at

https://www.godaddy.com/whois/results.aspx?domain=SMARTBEAR.COM
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=SMARTBEAR.COM
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=SMARTBEAR.COM
Name Server: NS-431.AWSDNS-53.COM
Name Server: NS-1701.AWSDNS-20.CO.UK
Name Server: NS-1416.AWSDNS-49.ORG
Name Server: NS-917.AWSDNS-50.NET
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-01-06T23:05:44Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

Sublist3r

sublist3r -d [   ]   SmartBear

image.png
image not found or type unknown

VPN   Staging

image.png
image not found or type unknown

OneForAll

https://github.com/shmilylty/OneForAll

python3 oneforall.py --target [ ]

image.png
image.png not found or type unknown

```
└─# python3 oneforall.py --target smartbear.com --fmt json run


OneForAll is a powerful subdomain integration tool


         ___            _ _
 ___ ___ ___|   _| ___ ___ ___| | | {v0.4.5 #dev}
| . |   | -_|   _| . |   _| .'| | |
|___|_|_|___|_| |___|_| |_,|_|_| git.io/fjHT1



OneForAll is under development, please update before each use!


[*] Starting OneForAll @ 2023-01-06 14:58:25


14:58:25,352 [INFOR] utils:523 - Checking dependent environment
14:58:25,353 [INFOR] utils:535 - Checking network environment
14:58:25,519 [INFOR] utils:546 - Checking for the latest version
14:58:25,634 [INFOR] utils:570 - The current version v0.4.5 is already the latest version
14:58:25,635 [INFOR] oneforall:243 - Start running OneForAll
14:58:25,636 [INFOR] oneforall:248 - Got 1 domains
14:58:25,648 [INFOR] wildcard:108 - Detecting smartbear.com use wildcard dns record or not
14:58:25,757 [ALERT] wildcard:123 - The domain smartbear.com disables wildcard
14:58:25,758 [INFOR] collect:44 - Start collecting subdomains of smartbear.com
14:58:25,805 [INFOR] module:63 - QueryMX module took 0.0 seconds found 0 subdomains
14:58:25,830 [INFOR] module:63 - NSECCheck module took 0.1 seconds found 0 subdomains
14:58:25,844 [INFOR] module:63 - QueryNS module took 0.0 seconds found 0 subdomains
14:58:25,846 [INFOR] module:63 - QuerySPF module took 0.0 seconds found 0 subdomains
14:58:25,869 [INFOR] module:63 - QuerySOA module took 0.1 seconds found 0 subdomains
14:58:25,875 [INFOR] module:63 - AXFRCheck module took 0.1 seconds found 0 subdomains
14:58:25,966 [INFOR] module:63 - CertInfo module took 0.2 seconds found 1 subdomains
14:58:25,983 [INFOR] module:63 - SiteDossierQuery module took 0.2 seconds found 11 subdomains
14:58:26,041 [INFOR] module:63 - QueryTXT module took 0.2 seconds found 0 subdomains
14:58:26,090 [ALERT] utils:273 - GET
https://transparencyreport.google.com/transparencyreport/api/v3/httpsreport/ct/certsearch?incl
ude_expired=true&include_subdomains=true&domain=smartbear.com 404 - Not Found 1611
14:58:26,090 [INFOR] module:63 - GoogleQuery module took 0.3 seconds found 0 subdomains
14:58:26,096 [ALERT] utils:273 - GET
https://fullhunt.io/api/v1/domain/smartbear.com/subdomains 401 - Unauthorized 50
14:58:26,096 [ALERT] utils:282 - {'message': 'Unauthorized access', 'success': False}
```

14:58:26,097 [INFOR] module:63 - FullHuntAPIQuery module took 0.3 seconds found 0 subdomains
14:58:26,099 [ALERT] utils:273 - GET https://jldc.me/anubis/subdomains/smartbear.com 300 - Multiple Choices 2
14:58:26,099 [ALERT] utils:282 - []
14:58:26,102 [INFOR] module:63 - AnubisQuery module took 0.3 seconds found 0 subdomains
14:58:26,122 [ALERT] utils:273 - GET
https://www.virustotal.com/ui/domains/smartbear.com/subdomains?limit=40&cursor= 429 - Too Many
Requests 181
14:58:26,122 [ALERT] utils:282 - {'error': {'message': 'Please re-send request with a valid
reCAPTCHA response in the "x-recaptcha-response" header', 'code': 'RecaptchaRequiredError'}}
14:58:26,125 [INFOR] module:63 - VirusTotalQuery module took 0.3 seconds found 0 subdomains
14:58:26,154 [ALERT] utils:273 - GET
https://api.threatminer.org/v2/domain.php?q=smartbear.com&rt=5 500 - Internal Server Error 0
14:58:26,155 [INFOR] module:63 - ThreatMinerQuery module took 0.3 seconds found 0 subdomains
14:58:26,231 [INFOR] module:63 - RiddlerQuery module took 0.4 seconds found 11 subdomains
14:58:26,234 [INFOR] module:63 - RapidDNSQuery module took 0.4 seconds found 144 subdomains
14:58:26,412 [INFOR] module:63 - HackerTargetQuery module took 0.6 seconds found 59 subdomains
14:58:26,438 [INFOR] module:63 - CSPCheck module took 0.7 seconds found 0 subdomains
14:58:26,837 [INFOR] module:63 - IP138Query module took 1.0 seconds found 5 subdomains
14:58:27,004 [ALERT] utils:273 - GET
https://searchdns.netcraft.com/?restriction=site+contains&position=limited&host=%2A.smartbear.
com&from=1 403 - Forbidden 9000
14:58:27,005 [INFOR] module:63 - NetCraftQuery module took 1.2 seconds found 0 subdomains
14:58:27,195 [INFOR] module:63 - SitemapCheck module took 1.4 seconds found 1 subdomains
14:58:27,268 [INFOR] module:63 - DNSDumpsterQuery module took 1.5 seconds found 58 subdomains
14:58:27,479 [INFOR] module:63 - BingSearch module took 1.6 seconds found 1 subdomains
14:58:27,568 [INFOR] module:63 - CertSpotterQuery module took 1.8 seconds found 68 subdomains
14:58:27,684 [INFOR] module:63 - SogouSearch module took 1.8 seconds found 1 subdomains
14:58:27,998 [INFOR] module:63 - ChinazQuery module took 2.2 seconds found 6 subdomains
14:58:28,049 [INFOR] module:63 - RobotsCheck module took 2.3 seconds found 0 subdomains
14:58:28,124 [INFOR] module:63 - CrossDomainCheck module took 2.3 seconds found 0 subdomains
14:58:28,380 [INFOR] module:63 - GiteeSearch module took 2.5 seconds found 0 subdomains
14:58:28,642 [INFOR] module:63 - CeBaiduQuery module took 2.8 seconds found 0 subdomains
14:58:28,749 [INFOR] module:63 - YahooSearch module took 2.9 seconds found 3 subdomains
14:58:28,965 [ALERT] utils:273 - GET https://api.sublist3r.com/search.php?domain=smartbear.com
523 - 7140
14:58:28,967 [INFOR] module:63 - Sublist3rQuery module took 3.2 seconds found 0 subdomains
14:58:29,026 [INFOR] module:63 - BaiduSearch module took 3.2 seconds found 0 subdomains
14:58:29,066 [INFOR] module:63 - SoSearch module took 3.2 seconds found 1 subdomains
14:58:29,302 [INFOR] module:63 - AlienVaultQuery module took 3.5 seconds found 56 subdomains

```
14:58:29,347 [INFOR] module:63 - AskSearch module took 3.5 seconds found 2 subdomains
14:58:30,856 [INFOR] module:63 - CrtshQuery module took 5.1 seconds found 155 subdomains
14:58:32,591 [INFOR] module:63 - YandexSearch module took 6.7 seconds found 0 subdomains
14:58:34,317 [INFOR] module:63 - RobtexQuery module took 8.5 seconds found 3 subdomains
14:58:38,971 [INFOR] module:63 - GoogleSearch module took 13.1 seconds found 5 subdomains
14:58:39,419 [ERROR] module:159 - HTTPSConnectionPool(host='www.dnsscan.cn', port=443): Read
timed out. (read timeout=13)
14:58:39,419 [INFOR] module:63 - QianXunQuery module took 13.6 seconds found 0 subdomains
14:58:39,678 [INFOR] module:63 - BruteSRV module took 0.3 seconds found 0 subdomains
14:58:39,683 [INFOR] brute:461 - Start running Brute module
14:58:39,684 [INFOR] brute:411 - Blasting smartbear.com
14:58:39,684 [INFOR] brute:119 - Querying NS records of smartbear.com
14:58:39,714 [INFOR] brute:129 - smartbear.com's authoritative name server is ['ns-
1416.awsdns-49.org.', 'ns-1701.awsdns-20.co.uk.', 'ns-431.awsdns-53.com.', 'ns-917.awsdns-
50.net.']

14:58:39,714 [INFOR] brute:99 - Querying A record from authoritative name server: ['ns-
1416.awsdns-49.org.', 'ns-1701.awsdns-20.co.uk.', 'ns-431.awsdns-53.com.', 'ns-917.awsdns-
50.net.']

14:58:39,823 [INFOR] brute:114 - Authoritative name server A record result:
['205.251.197.136', '205.251.198.165', '205.251.193.175', '205.251.195.149']
14:58:39,824 [INFOR] brute:348 - Generating dictionary for smartbear.com
14:58:39,913 [ALERT] utils:686 - Please check whether pirat.smartbear.com is correct or not
14:58:39,916 [INFOR] brute:366 - Dictionary size: 95247
14:58:39,957 [INFOR] brute:442 - Running massdns to brute subdomains
14:59:16,330 [INFOR] brute:197 - Counting IP cname appear times
14:59:16,332 [INFOR] brute:238 - Processing result
14:59:16,335 [ALERT] brute:452 - Brute module takes 36.7 seconds, found 71 subdomains of
smartbear.com
14:59:16,341 [INFOR] brute:492 - Finished Brute module to brute smartbear.com
14:59:16,354 [INFOR] resolve:143 - Start resolving subdomains of smartbear.com
14:59:16,375 [INFOR] resolve:166 - Running massdns to resolve subdomains
14:59:19,421 [INFOR] resolve:104 - Processing resolved results
14:59:19,437 [INFOR] resolve:172 - Finished resolve subdomains of smartbear.com
14:59:19,438 [INFOR] resolve:61 - Saving resolved results
14:59:19,452 [INFOR] request:258 - Start requesting subdomains of smartbear.com
14:59:19,453 [INFOR] request:39 - Port range:[80, 443]
14:59:19,456 [INFOR] request:56 - Generating request urls
14:59:19,456 [INFOR] request:217 - Requesting urls in bulk
```

```
Request Progress: 319it[01:20,  3.94it/s]
15:00:40,386 [INFOR] request:264 - Found that smartbear.com has 197 alive subdomains
15:00:40,387 [INFOR] finder:23 - Start Finder module
0it[00:00, ?it/s]15:00:40,664 [INFOR] request:217 - Requesting urls in bulk
Request Progress: 148it[00:04, 34.65it/s]
0it[00:00, ?it/s]15:00:45,140 [INFOR] module:63 - Finder module took 4.8 seconds found 0
subdomains
15:00:45,140 [INFOR] module:63 - Finder module took 4.8 seconds found 0 subdomains
15:00:45,141 [INFOR] resolve:143 - Start resolving subdomains of smartbear.com
15:00:45,141 [INFOR] request:258 - Start requesting subdomains of smartbear.com
15:00:45,142 [INFOR] request:39 - Port range:[80, 443]
15:00:45,142 [INFOR] request:56 - Generating request urls
15:00:45,142 [INFOR] request:217 - Requesting urls in bulk
Request Progress: 1it[00:00, 294.67it/s]
15:00:45,147 [INFOR] request:264 - Found that smartbear.com has 197 alive subdomains
15:00:45,148 [INFOR] altdns:203 - Start altdns module
15:00:45,620 [INFOR] altdns:210 - The altdns module generated 167 new subdomains
15:00:45,621 [INFOR] resolve:143 - Start resolving subdomains of smartbear.com
15:00:45,664 [INFOR] resolve:166 - Running massdns to resolve subdomains
15:00:47,222 [INFOR] resolve:104 - Processing resolved results
15:00:47,240 [INFOR] resolve:172 - Finished resolve subdomains of smartbear.com
15:00:47,251 [INFOR] request:258 - Start requesting subdomains of smartbear.com
15:00:47,251 [INFOR] request:39 - Port range:[80, 443]
0it[00:00, ?it/s]15:00:47,253 [INFOR] request:56 - Generating request urls
15:00:47,254 [INFOR] request:217 - Requesting urls in bulk
Request Progress: 97it[01:23,  1.16it/s]
15:02:10,733 [INFOR] request:264 - Found that smartbear.com has 219 alive subdomains
15:02:12,255 [ALERT] export:64 - The subdomain result for smartbear.com:
/opt/OneForAll/results/smartbear.com.json
15:02:12,257 [INFOR] oneforall:257 - Finished OneForAll
```

csv   json

└─# cat results/smartbear.com.json
[{"id": 137, "alive": 1, "request": 1, "resolve": 1, "url": "http://academy.smartbear.com", "subdomain": "academy.smartbear.com", "level": 1, "cname": "lu-elb-prod02-ssl-1936357760.eu-west-1.elb.amazonaws.com,lu-elb-prod02-ssl-1936357760.eu-west-1.elb.amazonaws.com,lu-elb-prod02-ssl-1936357760.eu-west-1.elb.amazonaws.com", "ip": "54.155.72.54,34.240.41.94,18.202.131.230", "public": "1,1,1", "cdn": 1, "port": 80, "status": 200, "reason": "OK", "title": "SmartBear Academy", "banner": "nginx", "cidr": "54.155.0.0/16,34.240.0.0/13,18.202.0.0/15", "asn": "AS16509,AS16509,AS16509", "org": "AMAZON-02,AMAZON-02,AMAZON-02", "addr": "\u7f8e\u56fd\u5f17\u5409\u5c3c\u4e9a\u963f\u4ec0\u672c,\u7231\u5c14\u5170Dublin,\u7231\u5c14\u5170Dublin", "isp": "\u4e9a\u9a6c\u900a,\u4e9a\u9a6c\u900a,\u4e9a\u9a6c\u900a", "source": "RapidDNSQuery"}, {"id": 138, "alive": 1, "request": 1, "resolve": 1, "url": "https://academy.smartbear.com", "subdomain": "academy.smartbear.com", "level": 1, "cname": "lu-elb-prod02-ssl-1936357760.eu-west-1.elb.amazonaws.com,lu-elb-prod02-ssl-1936357760.eu-west-1.elb.amazonaws.com,lu-elb-prod02-ssl-1936357760.eu-west-1.elb.amazonaws.com", "ip": "54.155.72.54,34.240.41.94,18.202.131.230", "public": "1,1,1", "cdn": 1, "port": 443, "status": 200, "reason": "OK", "title": "SmartBear Academy", "banner": "nginx", "cidr": "54.155.0.0/16,34.240.0.0/13,18.202.0.0/15", "asn": "AS16509,AS16509,AS16509", "org": "AMAZON-02,AMAZON-02,AMAZON-02", "addr": "\u7f8e\u56fd\u5f17\u5409\u5c3c\u4e9a\u963f\u4ec0\u672c,\u7231\u5c14\u5170Dublin,\u7231\u5c14\u5170Dublin", "isp": "\u4e9a\u9a6c\u900a,\u4e9a\u9a6c\u900a,\u4e9a\u9a6c\u900a", "source": "RapidDNSQuery"}, {"id": 265, "alive": 0, "request": 0, "resolve": 1, "url": "http://accounts.ftr.smartbear.c

Revision #6
Created 5 September 2022 03:00:16 by
Updated 19 June 2023 11:52:21 by