

ThreatQuotient



Team Cymru Recon CDF Guide

Version 1.0.0

June 07, 2021

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2021 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Contents

Versioning.....	5
Introduction.....	6
Installation	7
Configuration.....	8
ThreatQ Mapping.....	9
Team Cymru Recon	9
Team Cymru Recon Details (Supplemental):.....	10
Query Type Mapping.....	18
.query_type is apt_dns	21
.query_type is apt_dnsrr	21
.query_type is apt_hostname	22
.query_type is apt_ip	22
.query_type is banners.....	22
.query_type is banners_ptr.....	23
.query_type is bars_controllers.....	23
.query_type is bars_victims	24
.query_type is beacons	25
.query_type is compromised_hosts	25
.query_type is conpot_honeypot	26
.query_type is cookies.....	26
.query_type is cowrie_honeypot.....	27
.query_type is darknet	27
.query_type is ddos_attacks	28
.query_type is ddos_commands	29
.query_type is dionaea_honeypot	30
.query_type is dns_derived_domains_via_domain	30
.query_type is dns_derived_domains_via_ip	31
.query_type is dns_derived_ips_via_domain	31
.query_type is dns_derived_ips_via_ip	32
.query_type is dns_query.....	32
.query_type is dns_fingerprint	33
.query_type is flows.....	33
.query_type is malware_sandbox	34
.query_type is nmap_dnsrr.....	35
.query_type is nmap_fingerprint	35
.query_type is nmap_port.....	35
.query_type is ntp_server	36
.query_type is open_ports	36
.query_type is open_resolvers	37
.query_type is pdns	37
.query_type is pdns_nxd	38
.query_type is pdns_other	38
.query_type is portscan.....	39
.query_type is rdp_traffic.....	40
.query_type is router	41
.query_type is scanner	41
.query_type is sip	42
.query_type is snmp	43
.query_type is spam_domains	44
.query_type is spam_headers	44
.query_type is ssh	45

.query_type is tor	45
.query_type is urls	47
.query_type is useragents.....	48
.query_type is x509.....	49
Average Feed Run	51
Change Log	52

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions $\geq$ 4.34.0

Introduction

The Team Cymru Recon CDF ingests indicator objects published by Team Cymru from the following endpoint:

- <https://augury5.cymru.com/api/jobs>

Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable the feed](#).

Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).



If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Team Cymru Recon API Key used for authentication.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Team Cymru Recon

Main feed used to retrieve job ids which will further on be used in the Team Cymru Recon supplemental feed.

GET <https://augury5.cymru.com/api/jobs>

```
{
  {
    "current_page": 1,
    "data": [
      {
        "id": 994822,
        "name": "zombieants.biz",
        "description": "FQDN Search: zombieants.biz",
        "user_id": 46605,
        "username": "wchiange",
        "organization_id": 42970,
        "organization_name": "ThreatQ",
        "group_id": null,
        "group_name": null,
        "input": "{\n  \"uuid\": \"8c06b5ed-0b5c-4b30-8cc5-663abc530626\", \"limit\": 2000000, \"queries\": [\n    {\n      \"ptr\": \"zombieants.biz\", \"query_type\": \"banners_ptr\", \"qname\": \"zombieants.biz\", \"query_type\": \"dns_query\", \"dnsrr\": \"zombieants.biz\", \"query_type\": \"nmap_dnsrr\", \"qname\": \"zombieants.biz\", \"query_type\": \"pdns\", \"qname\": \"zombieants.biz\", \"query_type\": \"pdns_nxd\", \"hostname\": \"zombieants.biz\", \"query_type\": \"pdns_other\", \"dnsrr\": \"zombieants.biz\", \"query_type\": \"apt_dns\", \"dnsrr\": \"zombieants.biz\", \"query_type\": \"apt_dnsrr\", \"hostname\": \"zombieants.biz\", \"query_type\": \"apt_hostname\", \"query_type\": \"ddos_attacks\", \"target_hostname\": \"zombieants.biz\", \"query_type\": \"ddos_commands\", \"target_hostname\": \"zombieants.biz\", \"hostname\": \"zombieants.biz\", \"query_type\": \"bars_controllers\", \"query_type\": \"dns_derived_domains_via_domain\", \"query_domain\": \"zombieants.biz\", \"query_type\": \"dns_derived_ips_via_domain\", \"query_domain\": \"zombieants.biz\", \"hostname\": \"zombieants.biz\", \"query_type\": \"x509\", \"hostname\": \"zombieants.biz\", \"query_type\": \"malware_sandbox\", \"fqdn\": \"zombieants.biz\", \"query_type\": \"spam_domains\", \"url\": \"zombieants.biz\", \"query_type\": \"urls\"], \"timeout\": 14400, \"end_date\": \"12/16/2020 20:15:18\", \"job_name\": \"zombieants.biz\", \"start_date\": \"12/17/2019 20:15:18\", \"system_origin\": \"api\", \"limit_realtime\": 2000000, \"job_description\": \"FQDN Search: zombieants.biz\", \"limit_flowsonar\": 2000000\", \"total_bytes\": 155648, \"origin\": \"api\", \"updated_at\": \"2020-12-16 20:24:55\", \"created_at\": \"2020-12-16 20:15:21\", \"scheduled_interval\": [], \"status\": \"Completed\"
    },
    ....
  ]
}
```



No field is mapped from the main feed response. The `.id` field is used for the supplemental call.

Team Cymru Recon Details (Supplemental):

Supplemental feed called once per each job id returned by the Team Cymru Recon feed.

GET <https://augury5.cymru.com/api/jobs/{id}>

```
{"start_time":"2020-10-30
06:40:22","src_ip_addr":"104.248.88.112","src_cc":"NL","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":45647,"dst_port":80,"tcp_flags":2,"num_pkts":4,"num_octets":
240,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-10-30
11:38:06","src_ip_addr":"145.220.24.215","src_cc":"NL","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
17,"src_port":43395,"dst_port":53,"tcp_flags":0,"num_pkts":1,"num_octets":
73,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-10-31
15:34:48","src_ip_addr":"139.59.245.162","src_cc":"SG","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":31337,"dst_port":1287,"tcp_flags":2,"num_pkts":8192,"num_octets":
327680,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-10-31
15:34:48","src_ip_addr":"139.59.245.162","src_cc":"SG","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":31337,"dst_port":1088,"tcp_flags":2,"num_pkts":3000,"num_octets":
120000,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-06
17:37:08","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"27.147.131.150","dst_cc":"BD","proto":
6,"src_port":80,"dst_port":44367,"tcp_flags":25,"num_pkts":2,"num_octets":
553,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-09
22:32:33","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"192.241.234.142","dst_cc":"US","proto":
6,"src_port":587,"dst_port":37890,"tcp_flags":18,"num_pkts":8192,"num_octets":
393216,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-10
09:28:43","src_ip_addr":"145.220.0.46","src_cc":"NL","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
17,"src_port":26592,"dst_port":3544,"tcp_flags":0,"num_pkts":1,"num_octets":
68,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-12
01:15:08","src_ip_addr":"128.199.105.148","src_cc":"SG","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":45458,"dst_port":22,"tcp_flags":16,"num_pkts":8192,"num_octets":
425984,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-13
11:42:25","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"103.16.26.160","dst_cc":"HK","proto":
6,"src_port":21746,"dst_port":9001,"tcp_flags":2,"num_pkts":1,"num_octets":
40,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-14
11:53:00","src_ip_addr":"104.248.126.166","src_cc":"US","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":58370,"dst_port":22,"tcp_flags":24,"num_pkts":8192,"num_octets":
557056,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-14
21:16:58","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"168.167.91.69","dst_cc":"BW","proto":
1,"src_port":0,"dst_port":778,"tcp_flags":0,"num_pkts":1,"num_octets":
68,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-14
22:30:34","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"165.227.164.190","dst_cc":"DE","proto":
6,"src_port":20264,"dst_port":65372,"tcp_flags":16,"num_pkts":3000,"num_octets":
120000,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-15
04:25:18","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"168.167.91.69","dst_cc":"BW","proto":
1,"src_port":0,"dst_port":778,"tcp_flags":0,"num_pkts":1,"num_octets":
```

```
68,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-16
00:19:07","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"168.167.91.69","dst_cc":"BW","proto":
1,"src_port":0,"dst_port":778,"tcp_flags":0,"num_pkts":1,"num_octets":
68,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-16
03:18:00","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"23.160.193.39","dst_cc":"US","proto":
1,"src_port":0,"dst_port":778,"tcp_flags":0,"num_pkts":1,"num_octets":
68,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-16
21:18:53","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"168.167.91.69","dst_cc":"BW","proto":
1,"src_port":0,"dst_port":778,"tcp_flags":0,"num_pkts":1,"num_octets":
68,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-17
02:17:21","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"167.71.225.166","dst_cc":"US","proto":
1,"src_port":0,"dst_port":778,"tcp_flags":0,"num_pkts":3000,"num_octets":
204000,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-17
12:50:44","src_ip_addr":"192.42.116.15","src_cc":"NL","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":60874,"dst_port":993,"tcp_flags":27,"num_pkts":10,"num_octets":
1139,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-17
14:02:11","src_ip_addr":"27.0.180.89","src_cc":"IN","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":62133,"dst_port":445,"tcp_flags":2,"num_pkts":1,"num_octets":
52,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-18
21:24:23","src_ip_addr":"87.120.254.105","src_cc":"BG","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":36286,"dst_port":22,"tcp_flags":2,"num_pkts":3,"num_octets":
180,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-19
00:37:39","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"167.172.49.139","dst_cc":"US","proto":
6,"src_port":22,"dst_port":48440,"tcp_flags":16,"num_pkts":8192,"num_octets":
425984,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"start_time":"2020-11-19
01:18:06","src_ip_addr":"31.184.254.94","src_cc":"RU","dst_ip_addr":"165.232.45.141","dst_cc":"US","proto":
1,"src_port":0,"dst_port":771,"tcp_flags":0,"num_pkts":8192,"num_octets":
720896,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"timestamp":"2020-10-20 19:00:01","dnsrr":"weather-
online.hopto.org","ip_addr":"58.158.177.102","cc":"JP","type":"A","ttl":60,"query_type":"apt_dns"}
{"start_time":"2020-11-19
22:26:49","src_ip_addr":"188.226.188.45","src_cc":"NL","dst_ip_addr":"31.184.254.94","dst_cc":"RU","proto":
6,"src_port":52372,"dst_port":22,"tcp_flags":17,"num_pkts":8192,"num_octets":
425984,"sample_algo":null,"sample_interval":null,"query_type":"flows"}
{"timestamp":"2020-03-02 10:59:58","dnsrr":"ftp.jpgdowngaussip.ddns.info","confidence":50,"query_type":"apt_dnsrr"}
{"timestamp":"2021-03-02 19:08:56","hostname":"http://send.mofa.ns01.info:53/update?
id=00528208","query_type":"apt_hostname"}
{"timestamp":"2020-01-01 00:14:19","ip_addr":"219.85.40.59","cc":"TW","query_type":"apt_ip"}
{"timestamp":"2020-11-30 23:10:01","ip_addr":"52.219.120.147","cc":"US","asn":"16509","ptr":"s3-website-us-
west-1.amazonaws.com","query_type":"banners_ptr"}
{"timestamp":"2021-03-22 23:55:01","ip_addr":"123.58.210.170","cc":"CN","port":22,"type":"ssh","data":{"\n
"banner" : "\SSH-2.0-OpenSSH_7.4",\n
"key_type" : "ssh_rsa",\n
"auth_list" : [\n
"publickey",\n
"password",\n
],\n
"key_fingerprint" : "e5:e4:1d:e6:02:5e:c2:2d:a2:cb:cb:bb:b3:d1:26:91",\n
"\n",
"sub_type":"Net:SSH2","asn":"","ssl":true,"query_type":"banners"}
{"hostname":"us-east-1-a.route.herokuapp.com","ip_addr":"18.211.160.51","cc":"US","proto":6,"port":
80,"controller_uri":"http://us-east-1-
a.route.herokuapp.com/","type":"http","family":"vertexnet","subfamily":"controller v1","first_seen":"2019-07-05
03:35:06","last_seen":"2020-03-01 05:50:34","active":false,"query_type":"bars_controllers"}
{"timestamp":"2021-03-30 02:37:27","host_ip_addr":"45.179.206.24","host_cc":"BR","proto":6,"port":
38485,"controller":"http://sonic4us.ru/http/
image.php","controller_ip_addr":"184.105.192.2","controller_cc":"US","controller_port":80,"reputation_score":
90,"asn":"269100","family":"smokeloader","subfamily":"controller v1","query_type":"bars_victims"}
```

```
{ "timestamp": "2021-03-27
00:00:28", "ip_addr": "134.122.113.222", "cc": "US", "asn": "14061", "comment": "ssh", "rir": "arin", "src_port": null, "malware":
null, "query_type": "compromised_hosts" }
{ "timestamp": "2021-03-27
00:00:30", "ip_addr": "135.125.23.66", "cc": "FR", "asn": "16276", "comment": "ssh", "rir": "ripence", "src_port": null, "malware":
null, "query_type": "compromised_hosts" } { "timestamp": "2021-01-03
07:38:24", "client_ip_addr": "183.2.200.133", "client_cc": "CN", "server_ip_addr": "47.246.16.254", "server_cc": "HK", "serve
r_comment": "download.alicdn.com.danuoyi.tbcache.com", "server_port": 80, "proto": 6, "query_type": "beacons" }
{ "timestamp": "2020-11-30 07:58:36", "src_ip_addr": "164.68.112.178", "src_cc": "DE", "src_port":
59943, "application_proto": "s7comm", "data": "{ \"type\": \"CONNECTION_LOST\" }", "query_type": "conpot_honeypot" }
{ "timestamp": "2020-06-29 07:38:15", "src_ip_addr": "45.125.65.118", "src_cc": "HK", "src_port":
34657, "dst_ip_addr": "208.112.30.120", "dst_cc": "US", "dst_port":
80, "host": "www.fabtechdrillingequipment.com", "uri": "GET /Contact-Us", "user_agent": "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36 Edge/
16.16299", "referer": "http://www.fabtechdrillingequipment.com/Contact-
Us", "language": null, "cookie": "dnn_IsMobile=False; language=en-
US", "cookie_sha1": "cfa3c4fbe0d5547397df85e6becf7bc400dffafa", "query_type": "cookies" }
{ "timestamp": "2020-09-18 15:44:21", "src_ip_addr": "31.184.254.94", "src_cc": "RU", "src_port": 8602, "dst_port":
23, "proto": 6, "length": null, "ip_version": 4, "query_type": "darknet" }
{ "start_time": "2021-03-14 00:00:02", "end_time": "2021-03-14 00:00:03", "commands": null, "credentials": "[ ]", "dst_port":
22, "logged_in": "{root,123}", "src_ip_addr": "45.227.255.205", "src_cc": "PA", "src_port":
65332, "unknown_commands": null, "query_type": "cowrie_honeypot" }
{ "begin_time": "2021-03-01 00:00:58", "end_time": "2021-03-01 00:00:58", "target_hostname": "tcp://
42.193.216.140:10002", "target_ip_addr": "42.193.216.140", "target_cc": "CN", "subtarget": null, "controller": "tcp://
www1.gggatat456.com:1522", "controller_ip_addr": "51.68.183.108", "controller_cc": "CN", "controller_port":
1522, "command": "Type: aux_ddos\nData:
KsHYjBInAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAABQAAAAIAAB4AwAA", "family": "xorddos", "subfamily": "controller v1", "query_type": "ddos_attacks" }
{ "results": null, "query_type": "ddos_commands" }
{ "observed_at": "2020-11-16
02:02:06", "fqdn": "215t8vwcjjo.cg12r.com", "message_id": "c49ab7ff4ca7428ea1843b3e85589f2402a98cb2b5c3248f3b0d9eb1de170
44cb", "query_type": "spam_domains" }
{ "timestamp": "2021-02-25 13:00:03", "application_proto": "pcap", "proto": "tcp", "connection_type": "reject", "dst_port":
33747, "src_ip_addr": "45.135.232.109", "src_cc": "RU", "src_port": 42234, "query_type": "dionaea_honeypot" }
{ "timestamp": "2020-12-08 20:32:52", "proto":
17, "src_ip_addr": "112.111.113.242", "src_cc": "US", "dst_ip_addr": "20.50.23.2", "dst_cc": "US", "qname": "worstyear2020.com
", "class": "IN", "type": "DS", "zone": "com", "query_type": "dns_query" }
{ "timestamp": "2020-09-11 00:00:00", "ip_addr": "110.180.243.61", "cc": "CN", "fingerprint": "TIMEOUT id unavailable
(query timed out)", "query_type": "dns_fingerprint" }
{ "start_time": "2020-10-30
11:38:06", "src_ip_addr": "145.220.24.215", "src_cc": "NL", "dst_ip_addr": "31.184.254.94", "dst_cc": "RU", "proto":
17, "src_port": 43395, "dst_port": 53, "tcp_flags": 0, "num_pkts": 1, "num_octets":
73, "sample_algo": null, "sample_interval": null, "query_type": "flows" }
{ "timestamp": "2021-04-01 00:02:40", "ip_addr": "154.182.117.254", "cc": "EG", "dnsrr": "host-154.182.254.117-
static.tedata.net", "query_type": "nmap_dnsrr" }
{ "timestamp": "2020-11-16 17:55:24", "ip_addr": "31.184.254.94", "cc": "RU", "os": "Host: splitstore; OS:
Unix", "query_type": "nmap_fingerprint" }
{ "timestamp": "2021-04-01 00:02:40", "ip_addr": "178.89.155.145", "cc": "KZ", "proto": "tcp", "port":
53, "service": "tcpwrapped", "version": "", "query_type": "nmap_port" }
{ "timestamp": "2021-04-20
00:14:59", "src_ip_addr": "5.89.44.199", "src_cc": "IT", "version": "4", "processor": "unknown", "system": "UNIX", "stratum":
5, "refid": "91.80.35.139", "refid_cc": "IT", "raw": "version=\\4\\", processor=\\unknown\\, system=\\UNIX\\, leap=0,
stratum=5, precision=-21, rootdelay=, rootdisp=, refid=91.80.35.139, reftime=0xE4289561.A7F8063A,
clock=0xE4289B83.A96FAA0B, peer=5271, tc=10, mintc=3, offset=, frequency=, sys_jitter=, clk_jitter=,
clk_wander=, "query_type": "ntp_server" }
{ "timestamp": "2021-04-02 04:34:56", "ip_addr": "168.233.48.220", "cc": "US", "proto": "tcp", "port":
179, "service": null, "data": null, "asn": "40380", "asname": "SIERRATRADINGPOST, US", "query_type": "open_ports" }
{ "timestamp": "2020-06-30
```

```
04:54:50", "src_ip_addr": "208.112.30.1", "src_cc": "", "proto": null, "section": "answer", "aa": null, "qname": "tommybishop.co
m", "class": "IN", "type": "A", "ttl": null, "rdata": "208.112.30.120", "rdata_cc": "US", "query_type": "pdns"}
{"timestamp": "2020-09-18
17:29:11", "src_ip_addr": "31.184.254.94", "src_cc": "RU", "dst_ip_addr": "31.184.254.95", "dst_cc": "US", "scan_type": "ports
can", "scan_msg": "TCP Filtered Portsweep", "connection_count": 31, "ip_count":
7, "ip_range": "149.9.145.178:149.9.226.126", "port_proto_count": 1, "port_proto_range": "23:23", "query_type": "portscan"}
{"timestamp": "2020-10-31 22:37:32", "client_ip_addr": "195.154.179.3", "client_port":
40717, "server_ip_addr": "54.252.239.180", "server_port":
3389, "client_cc": "FR", "server_cc": "AU", "client_name": null, "cookie": "EXAMPLE\
a", "client_build": null, "keyboard_layout": null, "desktop_width": null, "desktop_height": null, "requested_color_depth": nu
ll, "result": null, "security_protocol": null, "cert_type": null, "client_dig_product_id": null, "client_asn": "{12876}", "serv
er_asn": "{16509}", "query_type": "rdp_traffic"}
{"timestamp": "2020-01-08 23:03:05", "ip_addr": "175.29.143.106", "cc": "BD", "vendor": "Cisco
Systems", "os_version": null, "processor": null, "query_type": "router"}
{"ip_addr": "31.184.254.94", "cc": "RU", "proto": 6, "ports": "{23}", "interval_probes_unique_dst_ip":
56, "interval_probes_unique_ports": 1, "interval_slash8_visited": 3, "total_ips_probed":
56, "asn": "49505", "query_type": "scanner"}
{"timestamp": "2020-10-28
00:00:38", "src_ip_addr": "62.210.78.81", "src_cc": "FR", "dst_ip_addr": "38.229.70.92", "dst_cc": "US", "sip_response": "INVI
TE", "sip_response_code":
0, "server": null, "user_agent": null, "allow": null, "accept": null, "response": null, "from_display": "", "from_number": "81", "f
rom_ip_addr": "38.229.70.92", "from_cc": "US", "from_port": 5060, "to_display": "", "to_number": "901146842002926", "to_port":
5060, "to_ip_addr": "38.229.70.92", "to_cc": "US", "contact_display": "", "contact_number": "81", "contact_ip_addr": "62.210.7
8.81", "contact_cc": "FR", "contact_port": 61426, "session_owner": "81", "query_type": "sip"}
{"timestamp": "2020-06-24 08:24:37", "src_ip_addr": "93.174.93.133", "src_cc": "NL", "src_port":
40413, "dst_ip_addr": "208.112.30.120", "dst_cc": "US", "dst_port": 80, "url": "http://caaofbecmcc.org/
xmlrpc.php", "query_type": "urls"}
{"timestamp": "2021-01-07 01:00:01", "ip_addr": "41.139.235.243", "cc": "KE", "version": 2, "oid_string": "ipAdEntAddr.
41.139.235.243 = IPAddress: 41.139.235.243", "query_type": "snmp"}
{"timestamp": "2020-11-16 16:02:09", "ip_addr": "31.184.254.94", "cc": "RU", "hostname": "31.184.254.94", "port":
995, "cn": "splitastore.ru", "alt_names": "", "c": "XX", "o": "XX", "email": "root@splitastore.ru", "subject": "C=XX, ST=XX,
L=XX, O=XX, OU=XX, CN=splitastore.ru, emailAddress=root@splitastore.ru", "not_after": "2030-11-03
13:11:06", "not_before": "2020-11-05 13:11:06", "version": 2, "md5": "4C:75:AA:5B:7C:4F:03:67:F5:12:86:1E:B5:BF:
5F:B9", "sha1": "3C:16:E1:05:A1:3A:5C:AA:F4:6F:20:8E:76:9D:73:37:71:36:9D:37", "issuer": "C=XX, ST=XX, L=XX, O=XX,
OU=XX, CN=splitastore.ru,
emailAddress=root@splitastore.ru", "issuer_cn": "splitastore.ru", "issuer_c": "XX", "issuer_o": "XX", "sig_algo": "sha256Wit
hRSAEncryption", "serial": "CE37FFBE045E57C7", "pem": "-----BEGIN CERTIFICATE-----\nMIICyGCAjOgAwIBAgIJAM43/\
74EX1FHMA0GCSqGSIb3DQEBCwUAMH4xCzAJBgNVnABYTAhYMQswCQYDVQIDAJYwDELMAkGA1UEBwwCWFgxGzAJBgNVBAoMA1hYMQsw\nnCQYDVQQLD
AJYwDEXMBUGA1UEAwOc3BsaXRhc3RvcmlucnUxIjAgBgkqhkiG9w0B\nnCQEWE3Jvb3Rac3BsaXRhc3RvcmlucnUwHhcNMjMTMTMxMTA2WmcNMzA
xMTAz\nMTMxMTA2WjB+MQswCQYDVQGEwJYwDELMAkGA1UEAwCWFgxGzAJBgNVBAcMA1hY\nnMQswCQYDVQKDAJYwDELMAkGA1UECwwCWFgxGzAVBgN
VBAMMDnNwG10YXN0b3Jl\nLnJlM1M1IwIAYJKoZIhvcNAQkBFhNyY290QHNwG10YXN0b3JlLnJlM1M1GfMA0GCSqG\nsIb3DQEBAQUAA4GNADCBiQKBgQD
tHFd96KQvm\NkKhNc70cJYpZHGashb08uIxxh\nnecs6u9fZ2VUUCSwq0DQGWcVIn\
DCEq1aKQVod+S4ecgzN7S4ulxYrFBgUCkAJPk\nnSRmzyCcEFVIFEo0931qFxb+vrjLPxhmOMaNaeeM9XKgTsZdubUXDRXI\
cw46scQv\NHLAcowIDAQAB01AwTjAdBgNVHQ4EFgQU40umwYhXDFN2IYq5e85GN0x8gPowHwYD\nnVR0jBBgwFoAU40umwYhXDFN2IYq5e85GN0x8gPow
DAYDVROTBAAUwAwEB\
zANBgkq\nnhkiG9w0BAQsFAA0BgQASKbcAzq36yAU7nWLhZJsaZrf0eoPkuue17p5+BoKdVYG5\nnVqkfm122P7u7Whwco07N2ZQKMqXcybyPg4MMtdyLK
WF+f7XChzv81aRpXXf9VAnV\nnRWroLZ4KwP\oXvahWtN81ru1X7pdFbm1jXxOG70gKKx1kHdVXuyI3d4w62Tw==\n-----END
CERTIFICATE-----\n", "query_type": "x509"}
{"timestamp": "2020-06-28 06:19:43", "src_ip_addr": "95.143.193.125", "src_cc": "SE", "src_port":
41813, "x_forwarded_for": null, "via": null, "dst_ip_addr": "208.112.30.120", "dst_cc": "US", "dst_port":
80, "user_agent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3563.0 Safari/
537.36", "cpu": null, "languages": "en-US,en;q=0.9", "character_sets": null, "query_type": "useragents"}
{"begin_time": "2021-03-31 23:59:05", "end_time": "2021-03-31 23:59:05", "target_hostname": "tcp://\
103.122.92.135:80", "target_ip_addr": "103.122.92.135", "target_cc": "HK", "subtarget": null, "controller": "tcp://\
ppp.xxxatat456.com:6002", "controller_ip_addr": "51.89.70.86", "controller_cc": "YE", "controller_port":
6002, "command": "Type: aux_ddos\nData:
Z3pch1AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAQAAAAIAAAB4AwAA", "family": "xorddos", "subfamily": "controller v1", "query_type": "ddos_attacks"}
{"scan_timestamp": "2019-02-22
```


Team Cymru Recon CDF
Version 1.0.0

Team Cymru Recon CDF
Version 1.0.0

```
"tcp", "dst_ip_addr": "91.195.240.126", "dst_byte_transfer": 370, "src_byte_transfer": 360}, {"dst_cc": "US", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "151.101.114.2", "dst_byte_transfer": 0, "src_byte_transfer": 370}, {"dst_cc": "DE", "dst_port": 443, "protocol": "tcp", "dst_ip_addr": "172.217.21.233", "dst_byte_transfer": 61866, "src_byte_transfer": 2469}, {"dst_cc": "DE", "dst_port": 443, "protocol": "tcp", "dst_ip_addr": "172.217.22.109", "dst_byte_transfer": 2820, "src_byte_transfer": 1946}, {"dst_cc": "DE", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "172.217.22.3", "dst_byte_transfer": 2155, "src_byte_transfer": 684}, {"dst_cc": "VG", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "199.191.50.185", "dst_byte_transfer": 459, "src_byte_transfer": 375}, {"dst_cc": "US", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "104.17.206.66", "dst_byte_transfer": 316, "src_byte_transfer": 359}, {"dst_cc": "US", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "151.101.114.2", "dst_byte_transfer": 0, "src_byte_transfer": 363}, {"dst_cc": "DE", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "172.217.21.233", "dst_byte_transfer": 505, "src_byte_transfer": 348}, {"dst_cc": "DE", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "172.217.22.3", "dst_byte_transfer": 1439, "src_byte_transfer": 458}, {"dst_cc": "US", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "199.48.135.146", "dst_byte_transfer": 516, "src_byte_transfer": 376}, {"dst_cc": "US", "dst_port": 80, "protocol": "tcp", "dst_ip_addr": "208.112.30.120", "dst_byte_transfer": 291, "src_byte_transfer": 376}, {"dst_cc": "DE", "dst_port": 0, "protocol": "icmp", "dst_ip_addr": "216.58.208.34", "dst_byte_transfer": 32, "src_byte_transfer": 32}], "urls": [{"url": "http://importsports.net/Ling/canon/dut/CRW_1375-1600.jpg", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://importsports.net/Ling/canon/dut/CRW_1443-1600.jpg", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://lh3.ggpht.com/-5F-7pwPiaA4/TgCG83mPjvI/AAAAAAACKw/es8Y-OEEvY8/BUDEL%2525202011%252520010.JPG", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://img1.blogblog.com/img/icon18_email.gif", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm+IHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc/HIGOD+aUx0=", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://ocsp.pki.goog/GTSGIAG3/MEKwRzBFMEMwQTAJBgUrDgMCGGUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfgZ+uksCCAPdvb6v2PrR\\", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://ocsp.pki.goog/GTSGIAG3/MEKwRzBFMEMwQTAJBgUrDgMCGGUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfgZ+uksCCC6746+1A1A7\\", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm+IHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc/HIGOD+aUx0=", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://ocsp.pki.goog/GTSGIAG3/MEKwRzBFMEMwQTAJBgUrDgMCGGUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfgZ+uksCCBLM7xVZVoGy\\", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGGUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm+IHV2ccHsBqBt5ZtJot39wZhi4CDQHjqTAc/HIGOD+aUx0=", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://ocsp.pki.goog/GTSGIAG3/MEKwRzBFMEMwQTAJBgUrDgMCGGUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfgZ+uksCCBLM7xVZVoGy\\", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://moviespics.wcgame.ru/data/2011-07-18/used-cars-movie.jpg", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://www.hanzoautobuzz.com/v1/wp-content/uploads/nissan_gtr_2012_2.jpg", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://www.vwot.org/community/modules/Gallery/albums/albus88/IMG_1262.jpg", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootst1.cab", "method": "GET", "user_agent": "Microsoft-CryptoAPI/6.1\\", {"url": "http://www.catamountstadium.com/Images/Graham_Trudo_Pose-Mackey-Watts.JPG", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://keywebtracker.com/?if=1&scr_w=800&scr_h=600&blog=file:///C:/Users/Phil/AppData/Local/Temp/ebda05de6a897c855f89e18258e9ec34fe722aa4.html&ref=&l=cars", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://i51.tinypic.com/98u5bd.jpg", "method": "GET", "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\\", {"url": "http://www.1948chevy.com/images/
```



```
48sp-7.gif\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://www.bevscafe.com/wp-content/uploads/2011/06/BevsCoffeeCup.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://www.covercars.com/cars/pictures/high/130241.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://www.modifiedcars.com/pix/cars_high/24046_42827.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab\", \"method\": \"GET\", \"user_agent\": \"Microsoft-CryptoAPI/6.1\", {\"url\": \"http://i421.photobucket.com/albums/pp297/morganchoo/Image019.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://www.automotorblog.com/wp-content/uploads/2011/04/Dodge-Viper-V10-engine.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab\", \"method\": \"GET\", \"user_agent\": \"Microsoft-CryptoAPI/6.1\", {\"url\": \"http://tinypic.com/images/404.gif\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://static.wix.com/media/586508f831479308f3fc6602fb169207.wix_mp\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://i421.photobucket.com/albums/pp297/morganchoo/08022009107.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\", {\"url\": \"http://i47.photobucket.com/albums/f156/chiefski/P2110176.jpg\", \"method\": \"GET\", \"user_agent\": \"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)\"]], \"query_type\": \"malware_sandbox\"}\n{\"observed_at\": \"2021-02-23 00:00:02\", \"src_ip_addr\": \"69.75.148.206\", \"src_cc\": \"US\", \"src_port\": 33026, \"dst_port\": 25, \"from_name\": \"Kunlun Energy\", \"from_email\": \"shillallen@hotmail.com\", \"to_addrs\": \"Kaliyaha51@icloud.com\", \"cc_addrs\": \"\", \"rcpt_to_addrs\": \"Kaliyaha51@icloud.com\", \"subject\": \"Employment Opportunities Job\", \"message_id\": null, \"query_type\": \"spam_headers\"}\n{\"timestamp\": \"2021-05-11 22:05:45\", \"src_ip_addr\": null, \"src_cc\": \"\", \"proto\": null, \"section\": \"authority\", \"aa\": null, \"qname\": \"betterfuturekkp.com\", \"class\": \"IN\", \"type\": \"NS\", \"ttl\": null, \"rdata\": \"ns1.server04controlserver.co.in\", \"query_type\": \"pdns_other\"}\n{\"timestamp\": \"2021-03-17 21:00:00\", \"proto\": 17, \"src_ip_addr\": \"61.211.226.41\", \"src_cc\": \"JP\", \"dst_ip_addr\": \"209.160.0.11\", \"dst_cc\": \"US\", \"dst_port\": 53, \"qname\": \"0.0.160.209.in-addr.arpa\", \"class\": \"IN\", \"type\": \"A\", \"zone\": \"0.160.209.in-addr.arpa\", \"query_type\": \"pdns_nxd\"}\n{\"results\": null, \"query_type\": \"ddos_commands\"}\n{\"timestamp\": \"2021-05-11 12:38:10\", \"ip_addr\": \"91.90.155.70\", \"cc\": \"DE\", \"os_version\": \"Ubuntu-4ubuntu0.2\", \"ssh_version\": \"SSH-2.0-OpenSSH_8.2p1\", \"type\": \"ssh-rsa\", \"key\": \"AAAAB3NzaC1yc2EAAAADAQABAAQGDQKrRi2oN4006fcmYGHbtDSDQcr7QIClQXL0VnmfTnyj3ixxZhRYpjCYZQgIzHzetN+3EEy\\T0gKVKh2FhRE35fwj1znWm7U6JEZYir0e94jbW5pKw3MpYPBd50jK3WE\\y4txBnCN79V0NRm000KyV9s95Y7K89RdX6r+pE2Qx1l0Qd1HyakmsaV8R0Q0EDiZwXa13C3svRYSBkELNC076zB0Nvh58gqhZ88zddmyff0Csw9TX0rWN0nFORu0rpQuw5CBbmxRA0Iw+liq6VEreCCDCMZvKdHI9bNubo+2NaxMPtVs6bAB49A0etxAEIKlsR6EVGjL1Yr2j6zZyc6nazfqf1DElcpESK7IVxPBpFQbJ4bndNngkU+U1guq19wpKsrqWxgqmBY6nD16EM\\kDOSbe3tpJcvxU6v4fbuZ0vPQxGzhY1p6jOCCdx8EsPXdxFMP8NYQiXYORZ9J7P1CbFwfKdQuuER6+b2mvtkpgbRC3Ifgm5uFyrQFDSCWs=\", \"city\": null, \"asn\": \"41412\", \"add_timestamp\": \"2021-05-11 13:00:03\", \"query_type\": \"ssh\"}\n{\"timestamp\": \"2021-05-12 14:02:01\", \"router_name\": \"nestor00patof\", \"ip_addr\": \"144.172.153.165\", \"cc\": \"CA\", \"ipv6_addr\": null, \"ipv6_cc\": \"\", \"or_port\": 1337, \"dir_port\": 0, \"platform\": \"Linux\", \"bandwidth\": 292, \"uptime\": 2282367, \"fingerprint\": \"FFFB FB50 A83A 414C C21B 4CDA 93A9 674B 0047 05E8\", \"authority\": false, \"hs_dir\": false, \"exit\": false, \"fast\": true, \"guard\": false, \"named\": false, \"stable\": true, \"running\": true, \"valid\": true, \"v2_dir\": true, \"hibernating\": false, \"bad_exit\": false, \"version\": \"0.4.5.7\", \"portlist\": \"reject 1-65535\", \"contact\": \"nestor00patof@ptaaff.ca\", \"published\": \"2021-05-12 07:49:33\", \"weight\": 51, \"query_type\": \"tor\"}\n.....
```

Query Type Mapping

TEAM CYMRU QUERY_TYPE VALUE	THREATQ ATTRIBUTE VALUE
apt_dns	Team Cymru APT Threats DNS
apt_dnsrr	Team Cymru APT Threats DNS RR
apt_hostname	Team Cymru APT Threats Hostnames
apt_ip	Team Cymru APT Threats IPs
banners	Team Cymru Banners
banners_ptr	Team Cymru Banners PTR
bars_controllers	Team Cymru BARS Botnet Controllers
bars_victims	Team Cymru BARS Botnet Victims
beacons	Team Cymru Beacons
compromised_hosts	Team Cymru Compromised Hosts
conpot_honeypot	Team Cymru Conpot
cookies	Team Cymru Cookies
cowrie_honeypot	Team Cymru Cowrie
darknet	Team Cymru Darknet
ddos_attacks	Team Cymru BARS Observed DDoS Attacks

TEAM CYMRU QUERY_TYPE VALUE	THREATQ ATTRIBUTE VALUE
ddos_commands	Team Cymru Observed DDoS Attack Commands
dionaea_honeypot	Team Cymru Dionaea
dns_fingerprint	Team Cymru DNS Server Fingerprinting
dns_derived_domains_via_domain	Team Cymru DNS Derived Domains Via Domains
dns_derived_domains_via_ip	Team Cymru DNS Derived Domains Via IPs
dns_derived_ips_via_domain	Team Cymru DNS Derived IPs Via Domains
dns_derived_ips_via_ip	Team Cymru DNS Derived IPs Via IPs
dns_query	Team Cymru DNS Queries
flows	Team Cymru Network Flows
nmap_dnsrr	Team Cymru NMap Reverse DNS Lookups
nmap_fingerprint	Team Cymru NMap OS Fingerprinting
nmap_port	Team Cymru NMap Open Ports
ntp_server	Team Cymru NTP Server Info
open_ports	Team Cymru Open Ports
open_resolvers	Team Cymru Open Resolvers
pdns	Team Cymru PDNS

TEAM CYMRU QUERY_TYPE VALUE	THREATQ ATTRIBUTE VALUE
pdns_nxd	Team Cymru PDNS NXDomain
pdns_other	Team Cymru PDNS Other Records
portscan	Team Cymru Port Scan
rdp_traffic	Team Cymru RDP
router	Team Cymru Router Information
scanner	Team Cymru Scanner
sip	Team Cymru SIP Info
snmp	Team Cymru SNMP Info
spam_domains	Team Cymru Spam Domains
spam_headers	Team Cymru Spam Headers
ssh	Team Cymru SSH Info
tor	Team Cymru Tor Public
urls	Team Cymru URLs
useragents	Team Cymru UserAgents
x509	Team Cymru x509 Certs
malware_sandbox	Team Cymru Malware Sandbox

ThreatQ provides the following default mapping for this feed, based on the `.query_type` value of each line.



The attributes corresponding to each indicator are present after the row containing the actual indicator.

`.query_type` is `apt_dns`

If `.query_type` is `"apt_dns"`:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
<code>.dnsrr</code>	Related Indicator.Value	FQDN	'weather-online.hopto.org'	
<code>.query_type</code>	Related Indicator.Attribute	Query Type	'Team Cymru APT Threats DNS'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
<code>.ttl</code>	Related Indicator.Attribute	TTL	'60'	
<code>.type</code>	Related Indicator.Attribute	DNS Record Type	'A'	
<code>.ip_addr</code>	Related Indicator.Value	IP Address	'58.158.177.102'	
<code>.query_type</code>	Related Indicator.Attribute	Query Type	'Team Cymru APT Threats DNS'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
<code>.cc</code>	Related Indicator.Attribute	Country Code	'JP'	

`.query_type` is `apt_dnsrr`

If `.query_type` is `"apt_dnsrr"`:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
<code>.dnsrr</code>	Indicator.Value	FQDN	'ftp.jpgdowngaussip.ddns.info'	
<code>.query_type</code>	Indicator.Attribute	Query Type	'Team Cymru APT Threats DNS RR'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
<code>.confidence</code>	Indicator.Attribute	Confidence	'50'	

.query_type is apt_hostname

If .query_type is "apt_hostname":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.hostname	Indicator.Value	URL	'http://send.mofa.ns01.info:53/update?id=00528208'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru APT Threats Hostnames'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is apt_ip

If .query_type is "apt_ip":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'219.85.40.59'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru APT Threats IPs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'TW'	

.query_type is banners

If .query_type is "banners":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'123.58.210.170'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Banners'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'CN'	
.asn	Indicator.Attribute	ASN		
.port	Indicator.Attribute	Port	'22'	
.type	Indicator.Attribute	Type	'ssh'	
.sub_type	Indicator.Attribute	Sub-Type	'Net::SSH2'	

.query_type is banners_ptr

If .query_type is "banners_ptr":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'52.219.120.147'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Banners PTR'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'US'	
.asn	Indicator.Attribute	ASN	'16509'	
.ptr	Indicator.Attribute	PTR Record	's3-website-us-west-1.amazonaws.com'	

.query_type is bars_controllers

If .query_type is "bars_controllers":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED AT	EXAMPLES	NOTES
.ip_addr	Related Indicator.Value	IP Address	.first_seen	'18.211.160.51'	
.query_type	Related Indicator.Attribute	Query Type	.first_seen	'Team Cymru BARS Botnet Controllers'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Related Indicator.Attribute	Country Code	.first_seen	'US'	
.family	Related Indicator.Attribute	Malware Family	.first_seen	'vertexnet'	
.subfamily	Related Indicator.Attribute	Malware Sub-Family	.first_seen	'controller v1'	
.port	Related Indicator.Attribute	Port	.first_seen	'80'	
.proto	Related Indicator.Attribute	Protocol	.first_seen	'6'	
.type	Related Indicator.Attribute	Protocol Type	.first_seen	'http'	
.controller_uri	Related Indicator.Value	URL	.first_seen	'http://us-east-1-a.route.herokuapp.com/'	
.query_type	Related Indicator.Attribute	Query Type	.first_seen	'Team Cymru BARS Botnet Controllers'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED AT	EXAMPLES	NOTES
.hostname	Related Indicator.Value	FQDN	.first_seen	'us-east-1-a.route.herokuapp.com'	
.query_type	Related Indicator.Attribute	Query Type	.first_seen	'Team Cymru BARS Botnet Controllers'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is bars_victims

- If .query_type is "bars_victims":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.controller_ip_addr	Related Indicator.Value	IP Address	'184.105.192.2'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru BARS Botnet Victims'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.asn	Related Indicator.Attribute	ASN	'269100'	
.controller_cc	Related Indicator.Attribute	Country Code	'US'	
.controller	Related Indicator.Attribute	Controller	'http://sonic4us.ru/http/image.php'	
.controller_port	Related Indicator.Attribute	Port	'80'	
.family	Related Indicator.Attribute	Malware Family	'smokeloader'	
.subfamily	Related Indicator.Attribute	Malware Sub-Family	'controller v1'	
.host_ip_addr	Related Indicator.Value	IP Address	'45.179.206.24'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru BARS Botnet Victims'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.host_cc	Related Indicator.Attribute	Country Code	'BR'	
.proto	Related Indicator.Attribute	Protocol	'6'	

.query_type is beacons

If `.query_type` is "beacons":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.server_ip_addr	Related Indicator.Value	IP Address	'47.246.16.254'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Beacons'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.server_port	Related Indicator.Attribute	Port	'80'	
.server_comment	Related Indicator.Attribute	Server Comment	'download.alicdn.com.danuoyi.tbcache.com'	
.server_cc	Related Indicator.Attribute	Country Code	'HK'	
.proto	Related Indicator.Attribute	Protocol	'6'	
.client_ip_addr	Related Indicator.Value	IP Address	'183.2.200.133'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Beacons'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.client_cc	Related Indicator.Attribute	Country Code	'CN'	

.query_type is compromised_hosts

If `.query_type` is "compromised_hosts":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'135.125.23.66'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Compromised Hosts'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.asn	Indicator.Attribute	ASN	'16276'	
.comment	Indicator.Attribute	Comment	'ssh'	
.cc	Indicator.Attribute	Country Code	'FR'	
.malware	Indicator.Attribute	Malware Family	'null'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.rir	Indicator.Attribute	Regional Internet Registry	'ripence'	
.src_port	Indicator.Attribute	Port	'null'	

.query_type is conpot_honeypot

If .query_type is "conpot_honeypot":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'164.68.112.178'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Conpot'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.application_proto	Indicator.Attribute	Application Protocol	's7comm'	
.data	Indicator.Attribute	Data	'{"type": "CONNECTION_LOST"}'	
.src_cc	Indicator.Attribute	Country Code	'DE'	
.src_port	Indicator.Attribute	Port	'59943'	

.query_type is cookies

If .query_type is "cookies":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.dst_ip_addr	Related Indicator.Value	IP Address	'135.125.23.66'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Cookies'	
.dst_cc	Related Indicator.Attribute	Country Code	'HK'	
.dst_port	Related Indicator.Attribute	Port	'80'	
.host	Related Indicator.Value	FQDN or IP Address	'www.fabtechdrillingequipment.com'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Cookies'	
.language	Related Indicator.Attribute	Language	'null'	
.referer	Related Indicator.Attribute	Referer	'http://www.fabtechdrillingequipment.com/Contact-Us'	
.uri	Related Indicator.Attribute	URI	'GET /Contact-Us'	
.src_ip_addr	Related Indicator.Value	IP Address	'45.125.65.118'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Cookies'	
.src_cc	Related Indicator.Attribute	Country Code	'HK'	
.src_port	Related Indicator.Attribute	Port	'34657'	

.query_type is cowrie_honeypot

If `.query_type` is "cowrie_honeypot":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'45.227.255.205'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.query_type	Indicator.Attribute	Query Type	'Team Cymru Cowrie'	
.src_cc	Indicator.Attribute	Country Code	'PA'	
.src_port	Indicator.Attribute	Port	'65332'	
.dst_port	Indicator.Attribute	Destination Port	'22'	
.commands	Indicator.Attribute	Commands	'null'	
.credentials	Indicator.Attribute	Credentials	'[]'	
.logged_in	Indicator.Attribute	Logged In	'{root,123}'	
.unknown_commands	Indicator.Attribute	Unknown Commands	'null'	

.query_type is darknet

If `.query_type` is "darknet":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'31.184.254.94'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.query_type	Indicator.Attribute	Query Type	'Team Cymru Darknet'	
.src_cc	Indicator.Attribute	Country Code	'RU'	
.src_port	Indicator.Attribute	Port	'8602'	
.dst_port	Indicator.Attribute	Destination Port	'23'	
.ip_version	Indicator.Attribute	IP Version	'4'	
.length	Indicator.Attribute	Packet Length	'null'	
.proto	Indicator.Attribute	Protocol	'6'	

.query_type is ddos_attacks

If .query_type is "ddos_attacks":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.controller_ip_addr	Related Indicator.Value	IP Address	'51.68.183.108'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru BARS Observed DDoS Attacks'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.controller	Related Indicator.Attribute	Controller	'tcp://www1.gggatat456.com:1522'	
.controller_cc	Related Indicator.Attribute	Country Code	'CN'	
.controller_port	Related Indicator.Attribute	Port	'1522'	
.family	Related Indicator.Attribute	Malware Family	'xorddos'	
.subfamily	Related Indicator.Attribute	Malware Sub-Family	'controller'	
.subtarget	Related Indicator.Attribute	Sub-target	'null'	
.attack_command	Related Indicator.Attribute	Commands		
.controller_port	Related Indicator.Attribute	Port	'6002'	
.command	Related Indicator.Attribute	Commands	'Type: aux_ddos\nData: Z3pch1AAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAA AABQAAAAIAAAB4AwAA'	
.target_cc	Related Indicator.Attribute	Target Country Code	'CN'	
.target_hostname	Related Indicator.Value	FQDN	'tcp://42.193.216.140:10002'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru BARS Observed DDoS Attacks'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
				match is found, the indicator and corresponding attributes are not ingested.
.target_ip_addr	Related Indicator.Value	IP Address	'42.193.216.140'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru BARS Observed DDoS Attacks'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.target_cc	Related Indicator.Attribute	Target Country Code	'CN'	

.query_type is ddos_commands

If .query_type is "ddos_commands":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.controller_ip_addr	Related Indicator.Value	IP Address		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Observed DDoS Attack Commands'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.controller	Related Indicator.Attribute	Controller		
.controller_cc	Related Indicator.Attribute	Country Code		
.controller_port	Related Indicator.Attribute	Port		
.controller_type	Related Indicator.Attribute	Controller Type		
.subtarget	Related Indicator.Attribute	Sub-target		
.attack_command	Related Indicator.Attribute	Commands		
.target_hostname	Related Indicator.Value	FQDN		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Observed DDoS Attack Commands'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.target_ip_addr	Related Indicator.Value	IP Address		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Observed DDoS Attack Commands'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.target_cc	Related Indicator.Attribute	Target Country Code		

.query_type is dionaea_honeypot

If .query_type is "dionaea_honeypot":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'45.135.232.109'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Dionaea'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Indicator.Attribute	Country Code	'RU'	
.src_port	Indicator.Attribute	Port	'42234'	
.application_proto	Indicator.Attribute	Application Protocol	'pcap'	
.connection_type	Indicator.Attribute	Connection Type	'reject'	
.dst_port	Indicator.Attribute	Destination Port	'33747'	
.proto	Indicator.Attribute	Protocol	'tcp'	

.query_type is dns_derived_domains_via_domain

If .query_type is "dns_derived_domains_via_domain":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.query_term	Related Indicator.Value	FQDN		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived Domains Via Domains'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.related_domain	Related Indicator.Value	FQDN		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived Domains Via Domains'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is dns_derived_domains_via_ip

If .query_type is "dns_derived_domains_via_ip":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.query_term	Related Indicator.Value	FQDN		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived Domains Via IPs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.related_cc	Related Indicator.Attribute	Country Code		
.related_domain	Related Indicator.Value	FQDN		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived Domains Via IPs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is dns_derived_ips_via_domain

If .query_type is "dns_derived_ips_via_domain":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.query_term	Related Indicator.Value	FQDN or IP Address		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived IPs Via Domains'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.related_cc	Related Indicator.Attribute	Country Code		
.related_ip_addr	Related Indicator.Value	FQDN		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived IPs Via Domains'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is dns_derived_ips_via_ip

If .query_type is "dns_derived_ips_via_ip":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.query_term	Related Indicator.Value	FQDN or IP Address		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived IPs Via IPs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.query_term_cc	Related Indicator.Attribute	Country Code		
.related_ip_addr	Related Indicator.Value	IP Address		
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Derived IPs Via IPs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.related_cc	Related Indicator.Attribute	Country Code		

.query_type is dns_query

If .query_type is "dns_query":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.dst_ip_addr	Related Indicator.Value	IP Address	'20:50:23:2'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Queries'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dst_cc	Related Indicator.Attribute	Country Code	'US'	
.qname	Related Indicator.Value	FQDN	'worstyear2020.com'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Queries'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.proto	Related Indicator.Attribute	Protocol	'17'	
.type	Related Indicator.Attribute	DNS Record Type	'DS'	
.zone	Related Indicator.Attribute	Response Policy Zone	'com'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Related Indicator.Value	IP Address	'112:111:113:242'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru DNS Queries'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'US'	

.query_type is dns_fingerprint

If .query_type is "dns_fingerprint":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'110.180.243.61'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru DNS Server Fingerprinting'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'CN'	
.fingerprint	Indicator.Attribute	Fingerprint	'TIMEOUT id unavailable (query timed out)'	

.query_type is flows

If .query_type is "flows":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.dst_ip_addr	Related Indicator.Value	IP Address	'31.184.254.94'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Network Flows'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dst_cc	Related Indicator.Attribute	Country Code	'RU'	
.src_ip_addr	Related Indicator.Value	IP Address	'145.220.24.215'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Network Flows'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'NL'	

.query_type is malware_sandbox

If .query_type is "malware_sandbox":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.md5	Related Indicator.Value	MD5	'4657573a39e00e1774227a530135c3fd'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Malware Sandbox'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.sha1	Related Indicator.Value	SHA-1	'ebda05de6a897c855f89e18258e9ec34fe722aa4'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Malware Sandbox'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.sha256	Related Indicator.Value	SHA-256	'672a857e036c85364437210ca85ee88561a26cef631f27f58de68d21505ab815'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Malware Sandbox'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.connections[].dst_ip_addr	Related Indicator.Value	IP Address	'172.217.21.233'	
.connections[].dst_cc	Related Indicator.Attribute	Country Code	'DE'	
.connections[].protocol	Related Indicator.Attribute	Protocol	'tcp'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Malware Sandbox'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.urls[].url	Related Indicator.Value	URL	'http://importsports.net/Ling/canon/dut/CRW_1375-1600.jpg'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Malware Sandbox'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dns[].dnsrr	Related Indicator.Value	FQDN	'ocsp.pki.goog'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Malware Sandbox'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
				the indicator and corresponding attributes are not ingested.

.query_type is nmap_dnsrr

If `.query_type` is "nmap_dnsrr":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'154.182.117.254'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru NMap Reverse DNS Lookups'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'EG'	
.dnsrr	Indicator.Attribute	DNS Resource Record	'host-154.182.254.117-static.tedata.net'	

.query_type is nmap_fingerprint

If `.query_type` is "nmap_fingerprint":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'31.184.254.94'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru NMap OS Fingerprinting'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'RU'	
.os	Indicator.Attribute	Operating System	'Host: splitstore; OS: Unix'	

.query_type is nmap_port

If `.query_type` is "nmap_port":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'178.89.155.145'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru NMap Open Ports'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.cc	Indicator.Attribute	Country Code	'KZ'	
.service	Indicator.Attribute	Service	'tcpwrapped'	
.port	Indicator.Attribute	Port	'53'	
.proto	Indicator.Attribute	Protocol	'tcp'	

.query_type is ntp_server

If .query_type is "ntp_server":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'5.89.44.199'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru NTP Server Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Indicator.Attribute	Country Code	'IT'	
.processor	Indicator.Attribute	Processor	'unknown'	
.raw	Indicator.Attribute	Raw NTP Server Response	'version="4'	
.refid	Indicator.Attribute	NTP Reference ID	'91.80.35.139'	
.system	Indicator.Attribute	System	'UNIX'	
.version	Indicator.Attribute	NTP Version	'4'	

.query_type is open_ports

If .query_type is "open_ports":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'168.233.48.220'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Open Ports'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'US'	
.data	Indicator.Attribute	Data	'null'	
.port	Indicator.Attribute	Port	'179'	
.proto	Indicator.Attribute	Protocol	'tcp'	
.service	Indicator.Attribute	Service	'null'	
.asn	Indicator.Attribute	ASN	'40380'	
.asname	Indicator.Attribute	AS Name	'SIERRATRADINGPOST'	

.query_type is open_resolvers

If .query_type is "open_resolvers":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'168.233.48.220'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Open Resolvers'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Indicator.Attribute	Country Code	'US'	

.query_type is pdns

If .query_type is "pdns":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.qname	Related Indicator.Value	FQDN	'tommybishop.com'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.aa	Related Indicator.Attribute	Authoritative Answer	'null'	
.proto	Related Indicator.Attribute	Protocol	'null'	
.section	Related Indicator.Attribute	DNS Section	'answer'	
.ttl	Related Indicator.Attribute	TTL	'null'	
.type	Related Indicator.Attribute	Type	'A'	
.rdata	Related Indicator.Value	IP Address or FQDN	'208.112.30.120'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.rdata_cc	Related Indicator.Attribute	Country Code	'US'	
.src_ip_addr	Related Indicator.Value	IP Address	'208.112.30.1'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code		

.query_type is pdns_nxd

If `.query_type` is "pdns_nxd":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.qname	Related Indicator.Value	FQDN	'0.0.160.209.in-addr.arpa'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS NXDomain'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.type	Related Indicator.Attribute	Type	'A'	
.proto	Related Indicator.Attribute	Protocol	'17'	
.zone	Related Indicator.Attribute	Response Policy Zone	'0.160.209.in-addr.arpa'	
.type	Related Indicator.Attribute	DNS Record Type	'A'	
.src_ip_addr	Related Indicator.Value	IP Address	'61.211.226.41'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS NXDomain'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'JP'	
.dst_ip_addr	Related Indicator.Value	IP Address	'209.160.0.11'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS NXDomain'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dst_cc	Related Indicator.Attribute	Country Code	'US'	
.dst_port	Related Indicator.Attribute	Port	'53'	

.query_type is pdns_other

If `.query_type` is "pdns_other":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.qname	Related Indicator.Value	FQDN	'betterfuturekkp.com'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS Other Records'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.aa	Related Indicator.Attribute	Authoritative Answer	'null'	
.type	Related Indicator.Attribute	DNS Record Type	'NS'	
.proto	Related Indicator.Attribute	Protocol	'null'	
.ttl	Related Indicator.Attribute	TTL	'null'	
.section	Related Indicator.Attribute	DNS Section	'authority'	
.rdata	Related Indicator.Value	IP Address or FQDN	'ns1.server04controlserver.co.in'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS Other Records'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_ip_addr	Related Indicator.Value	IP Address	'null'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru PDNS Other Records'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is portscan

If .query_type is "portscan":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Related Indicator.Value	IP Address	'31.184.254.94'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Port Scan'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'RU'	
.ip_range	Related Indicator.Attribute	IP Range	'149.9.145.178:149.9.226.126'	
.port_proto_range	Related Indicator.Attribute	Port Range	'23:23'	
.scan_msg	Related Indicator.Attribute	Scan Message	'TCP Filtered Portsweep'	
.scan_type	Related Indicator.Attribute	Scan Type	'portscan'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.dst_ip_addr	Related Indicator.Value	IP Address	'31.184.254.95'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Port Scan'	
.dst_cc	Related Indicator.Attribute	Country Code	'US'	
.connection_count	Related Indicator.Attribute	Connection Count	'31'	

.query_type is rdp_traffic

If .query_type is "rdp_traffic":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.client_ip_addr	Related Indicator.Value	IP Address	'195.154.179.3'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru RDP'	
.client_cc	Related Indicator.Attribute	Country Code	'FR'	
.client_asn	Related Indicator.Attribute	ASN	'{12876}'	
.client_build	Related Indicator.Attribute	RDP Client Version	'RU'	
.client_dig_product_id	Related Indicator.Attribute	Digital Product ID	'null'	
.client_name	Related Indicator.Attribute	Name	'null'	
.client_port	Related Indicator.Attribute	Port	'40717'	
.cookie	Related Indicator.Attribute	Cookie	'EXAMPLE\A'	
.desktop_height	Related Indicator.Attribute	Remote Desktop Height	'null'	
.desktop_width	Related Indicator.Attribute	Remote Desktop Width	'null'	
.keyboard_layout	Related Indicator.Attribute	Remote Desktop Keyboard Layout	'null'	
.requested_color_depth	Related Indicator.Attribute	Remote Desktop Request Color Depth	'RU'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.server_ip_addr	Related Indicator.Value	IP Address	'54.252.239.180'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru RDP'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.server_cc	Related Indicator.Attribute	Country Code	'AU'	
.server_port	Related Indicator.Attribute	Port	'3389'	
.server_asn	Related Indicator.Attribute	ASN	'{16509}'	
.security_protocol	Related Indicator.Attribute	Security Protocol	'null'	

.query_type is router

If .query_type is "router":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'175.29.143.106'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Router Information'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'BD'	
.os_version	Indicator.Attribute	Operating System Version	'null'	
.processor	Indicator.Attribute	Processor	'null'	
.vendor	Indicator.Attribute	Vendor	'Cisco Systems'	

.query_type is scanner

If .query_type is "scanner":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'31.184.254.94'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Scanner'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'RU'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.asn	Indicator.Attribute	ASN	'49505'	
.interval_probes_unique_dst_ip	Indicator.Attribute	Unique Dest. IPs Probed	'56'	
.interval_probes_unique_ports	Indicator.Attribute	Unique Ports Scanned	'1'	
.interval_slash8_visited	Indicator.Attribute	Slash8 Visited	'3'	
.ports	Indicator.Attribute	Port	'{23}'	
.proto	Indicator.Attribute	Protocol	'6'	
.total_ips_probed	Indicator.Attribute	Total IPs Probed	'56'	

.query_type is sip

If .query_type is "sip":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.contact_ip_addr	Related Indicator.Value	IP Address	'62.210.78.81'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru SIP Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.contact_cc	Related Indicator.Attribute	Country Code	'FR'	
.contact_display	Related Indicator.Attribute	Display Name		
.contact_number	Related Indicator.Attribute	Contact Number	'81'	
.contact_port	Related Indicator.Attribute	Contact Port	'61426'	
.dst_ip_addr	Related Indicator.Value	IP Address	'38.229.70.92'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru SIP Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dst_cc	Related Indicator.Attribute	Country Code	'US'	
.from_ip_addr	Related Indicator.Value	IP Address	'38.229.70.92'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru SIP Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.from_cc	Related Indicator.Attribute	Country Code	'US'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.from_display	Related Indicator.Attribute	Display Name		
.from_number	Related Indicator.Attribute	Contact Number	'81'	
.from_port	Related Indicator.Attribute	Port	'5060'	
.src_ip_addr	Related Indicator.Value	IP Address	'62.210.78.81'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru SIP Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'FR'	
.to_ip_addr	Related Indicator.Value	IP Address	'38.229.70.92'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru SIP Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.to_cc	Related Indicator.Attribute	Country Code	'US'	
.to_display	Related Indicator.Attribute	Display Name		
.to_number	Related Indicator.Attribute	Contact Number	'901146842002926'	
.to_port	Related Indicator.Attribute	Port	'5060'	

.query_type is snmp

If .query_type is "snmp":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'41.139.235.243'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru SNMP Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'KE'	
.oid_string	Indicator.Attribute	OID String	'ipAdEntAddr. 41.139.235.243 = IpAddress: 41.139.235.243'	
.version	Indicator.Attribute	SNMP Version	'2'	

.query_type is spam_domains

If .query_type is "spam_domains":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.fqdn	Indicator.Value	FQDN	'215t8vwczo.cg12r.com'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Spam Domains'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is spam_headers

If .query_type is "spam_headers":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.src_ip_addr	Indicator.Value	IP Address	'69.75.148.206'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru Spam Headers'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc_addrs	Indicator.Attribute	Email Address		
.dst_port	Indicator.Attribute	Port	'25'	
.from_email	Indicator.Attribute	Email Address	'shil1allen@hotmail.com'	
.from_name	Indicator.Attribute	From Name	'"Kunlun Energy"'	
.rcpt_to_addrs	Indicator.Attribute	Email Address		
.src_cc	Indicator.Attribute	Country Code	'US'	
.src_port	Indicator.Attribute	Port	'33026'	
.subject	Indicator.Attribute	Email Subject		
.to_addrs	Indicator.Attribute	Email Subject	'Kaliyaha51@icloud.com'	

.query_type is ssh

If .query_type is "ssh":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Indicator.Value	IP Address	'91.90.155.70'	
.query_type	Indicator.Attribute	Query Type	'Team Cymru SSH Info'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.cc	Indicator.Attribute	Country Code	'DE'	
.city	Indicator.Attribute	City	'null'	
.key	Indicator.Attribute	SSH Key	'AAAAB3NzaC1yc2EAAAADAQABAAQgQDKrRi2oN4OO6fcMyYGHbtDSDqcr7QIClQXL0VnmfTnyj3ixxZhRYpjCYZQglzHzetN+3EEy/T0gKVKh2FhRE35fwj1znWm7U6JEZYir0e94jbW5pKw3MpYPBd5OjK3WE/y4txBnCn79V0NRm000KyV9s95Y7K89RdX6r+pE2Qxl1oQd1HyakmsaV8R0QOEDiZwXal3C3svRYSBkELNC076zB0Nvhh58gqhZ88zddmyff0CsW9TX0rWN0nF0Ru0rpQuw5CBbbmxRAolw+liq6VEreCCDCMZvWKDhI9bNubo+2NaxMPtVs6bAB49A0etxAelKlsR6EVGjL1Yr2j6zZyc6nazfqf1DElcpESK7IVxPBpFQbj4bndNnqkU+U1guql9wpKsrqWxgqmBY6nD16EM/kD0Sbe3tpjcvxU6v4fbuZOvPQxGzhYlp6jOCCdx8EsPXdxFMP8NYQiXYORZ9j7PICbFwfkQduuER6+b2mvtkpgbRC3lfgm5uFyrQFDSCWs='	
.os_version	Indicator.Attribute	OS Version	'Ubuntu-4ubuntu0.2'	
.ssh_version	Indicator.Attribute	SSH Version		
.type	Indicator.Attribute	SSH Key Type	'ssh-rsa'	
.asn	Indicator.Attribute	ASN	'41412'	

.query_type is tor

If .query_type is "tor":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ipv6_addr	Related Indicator.Value	IP Address	'null'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Tor Public'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.ipv6_cc	Related Indicator.Attribute	Country Code		
.ip_addr	Related Indicator.Value	IP Address	'144.172.153.165'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru Tor Public'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.authority	Related Indicator.Attribute	Authority	'false'	
.bad_exit	Related Indicator.Attribute	Bad Exit	'false'	
.bandwidth	Related Indicator.Attribute	Bandwidth	'292'	
.cc	Related Indicator.Attribute	Country Code	'CA'	
.contact	Related Indicator.Attribute	Contact	'nestor00patof@ptaff.ca'	
.dir_port	Related Indicator.Attribute	Port	'0'	
.exit	Related Indicator.Attribute	Exit	'false'	
.fast	Related Indicator.Attribute	Fast	'true'	
.fingerprint	Related Indicator.Attribute	Fingerprint	'FFFB FB50 A83A 414C C21B 4CDA 93A9 674B 0047 05E8'	
.guard	Related Indicator.Attribute	Guard	'false'	
.hibernating	Related Indicator.Attribute	Hibernating	'false'	
.hs_dir	Related Indicator.Attribute	HS Directory	'false'	
.named	Related Indicator.Attribute	Named	'false'	
.or_port	Related Indicator.Attribute	Port	'1337'	
.platform	Related Indicator.Attribute	Platform	'Linux'	
.router_name	Related Indicator.Attribute	Router Name	'nestor00patof'	
.running	Related Indicator.Attribute	Running	'true'	
.stable	Related Indicator.Attribute	Stable	'true'	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.v2_dir	Related Indicator.Attribute	v2 Directory Protocol	'true'	
.valid	Related Indicator.Attribute	Valid	'true'	
.version	Related Indicator.Attribute	Version	'0.4.5.7'	
.weight	Related Indicator.Attribute	Weight	'51'	

.query_type is urls

If `.query_type` is "urls":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.dst_ip_addr	Related Indicator.Value	IP Address	'208.112.30.120'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru URLs'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dst_cc	Related Indicator.Attribute	Country Code	'US'	
.dst_port	Related Indicator.Attribute	Port	'80'	
.src_ip_addr	Related Indicator.Value	IP Address	'93.174.93.133'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru URLs'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'NL'	
.src_port	Related Indicator.Attribute	Port	'40413'	
.url	Related Indicator.Value	URL	'http://caaofbecmcc.org/xmlrpc.php'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru URLs'	Maps the value of <code>.query_type</code> key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

.query_type is useragents

If .query_type is "useragents":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.dst_ip_addr	Related Indicator.Value	IP Address	'208.112.30.120'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru UserAgents'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.dst_cc	Related Indicator.Attribute	Country Code	'US'	
.dst_port	Related Indicator.Attribute	Port	'80'	
.src_ip_addr	Related Indicator.Value	IP Address	'95.143.193.125'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru UserAgents'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.src_cc	Related Indicator.Attribute	Country Code	'SE'	
.src_port	Related Indicator.Attribute	Port	'41813'	
.languages	Related Indicator.Attribute	Languages	'en-US,en;q=0.9'	
.user_agent	Related Indicator.Attribute	User-Agent	'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/ 537.36 (KHTML, like Gecko) Chrome/71.0.3563.0 Safari/537.36'	
.via	Related Indicator.Attribute	Via	'null'	
.x_forwarded_for	Related Indicator.Attribute	X-Forwarded For	'null'	
.character_sets	Related Indicator.Attribute	Character Sets	'null'	
.cpu	Related Indicator.Attribute	CPU	'null'	

.query_type is x509

If .query_type is "x509":

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.ip_addr	Related Indicator.Value	IP Address	'31.184.254.94'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru x509 Certs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.hostname	Related Indicator.Value	FQDN or IP Address	'31.184.254.94'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru x509 Certs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.
.altnames	Related Indicator.Attribute	Certificate Owner Alternate Common Name		
.cc	Related Indicator.Attribute	Country Code	'RU'	
.cn	Related Indicator.Attribute	Certificate Owner Common Name	'splitastore.ru'	
.email	Related Indicator.Attribute	Certificate Owner Email Address	'root@splitastore.ru'	
.issuer	Related Indicator.Attribute	Certificate Authority Signing Certificate	'C=XX, ST=XX, L=XX, O=XX, OU=XX, CN=splitastore.ru, emailAddress=root@splitastore.ru'	
.issuer_c	Related Indicator.Attribute	Certificate Authority Country	'XX'	
.issuer_cn	Related Indicator.Attribute	Issuer Common Name	'splitastore.ru'	
.issuer_o	Related Indicator.Attribute	Issuer Organization	'XX'	
.o	Related Indicator.Attribute	Certificate Owner Organization Name	'XX'	
.pem	Related Indicator.Attribute	PEM Certificate	'-----BEGIN CERTIFICATE-----\nMIICyJCCAjOgAwIBAgIJAM43/74EXIfHMA0GCSqGSIb3DQEB\nCwUAMH4xCzAJBgNVnBAYTA\nlhYMQswCQYDVQQIDAJYWDEL\nMAkGA1UEBwwCWFGxCzAJBgN\nVBAoMAIhYMQswCQYDVQQQL\nDAJYWDEXMBUGA1UEAwwOc3\nBsaXRhc3RvcnUucnUxIjAgBgkq\nhkiG9w0BnCQEWE3Jvb3RAC3Bs\naXRhc3RvcnUucnUwHhcNMjAx\nMTA1MTMxMTA2WhcNMzAxMT\nAz\nMTMxMTA2WjB+MQswCQYD	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
			VQQGEWjYWDELMAkGA1UECAwCWFgxZzAjBgNVBACMAIhYlnMQswCQYDVQQKDAjYWDELMAkGA1UECwwCWFGxFzAVBgNVBAMMDnNwbGl0YXN0b3JlLnJ1MSIwIAYJKoZIhvcNAQkBFhNyb290QHnwbGl0YXN0b3JlLnJ1MIGfMA0GCSqG\nSib3DQEBQUAA4GNADCBiQKBgQDdHfD96KQvm/NxKhG7OcjYpZHGashbO8ulxkh\\necs6u9fZ2VVUCSwq0DQGwCvIn/DCeq1aKVod+S4ecgzn2FS4ulx yrFBguCkAxJPK\\nSRmzyCcEFVIFeoo931qFxb+vrjLPxhmOMaNaeM9XKgTsZdubUXDRXI/cw46scQv\\nHLAcowIDAQABo1AwTjAdBgNVHQ4EFgQU40umwYhXDFN2IYq5e85GNOx8gPowHwYD\\nVR0jBBgwFoAU40umwYhXDFN2IYq5e85GNOx8gPowDAYDVR0TB AUwAwEB/zANBgkq\\nhkiG9w0BAQSF AAObgQASkbcAzq36yAU7nWLhzjsaZrf0eoPkuel7p5+BoKdVYG5\\nVqkfMI22P7u7WhwcoO7N22QKMqXcybyPg4M MTdyLKWF+f7XCHzv8laRpXXf9VAnV\\nRWroLZ4KWpP/oXvahWt2N81rulX7pdFbm1jXxOG7OgKKx1kHdVXuyI3d4w62Tw==\\n-----END CERTIFICATE-----\\n'	
.port	Related Indicator.Attribute	Port	'995'	
.serial	Related Indicator.Attribute	Serial	'CE37FFBE045E57C7'	
.sig_algo	Related Indicator.Attribute	Signature Algorithm	'sha256WithRSAEncryption'	
.subject	Related Indicator.Attribute	Certificate Owner Distinguished Name	'C=XX, ST=XX, L=XX, O=XX, OU=XX, CN=splitastore.ru, emailAddress=root@splitastore.ru'	
.sha1	Related Indicator.Value	SHA-1	'3C:16:E1:05:A1:3A:5C:AA:F4:6F:20:8E:76:9D:73:37:71:36:9D:37'	
.query_type	Related Indicator.Attribute	Query Type	'Team Cymru x509 Certs'	Maps the value of .query_type key to a string based on the Query Type Mapping below. If no match is found, the indicator and corresponding attributes are not ingested.

Average Feed Run

METRIC	RESULT
Run Time	5 hours
Indicators	44,398
Indicator Attributes	89,425



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Change Log

- Version 1.0.0
 - Initial release