Passive DNS

Archived: 2026-04-06 01:11:18 UTC

Passive DNS version 2.0

CIRCL Passive DNS is a database that stores historical DNS records from various resources, including malware analysis and partners. The DNS historical data is indexed, making it searchable for incident handlers, security analysts, or researchers.

In November 2023, CIRCL released version 2.0 of its Passive DNS service. The new version is backward-compatible with the previous 1.0 version. The output format remains Passive DNS - Common Output Format, and the query interface is similar. New headers were introduced to support some new functionalities, including filtering and pagination. If no headers are set, the Passive DNS API falls back to the previous 1.0 version's behavior.

Access to CIRCL Passive DNS

Access to CIRCL Passive DNS is restricted to trusted partners both in Luxembourg and abroad. If you are interested in gaining access, please contact us and provide details about your affiliation and the intended use of the Passive DNS data.

API documentation

How to Use the Service

CIRCL Passive DNS is accessible via a REST API, and the output format is in JSON following the Passive DNS - Common Output Format.

The REST API is accessible via the following URL:

```
https://www.circl.lu/pdns/query/<queryvalue>
```

Query values can be any records such as IP addresses, hostnames, or domain names (please note that CIDR block queries are not supported).

For example:

`https://www.circl.lu/pdns/query/circl.lu`

```
1{"rrtype": "A", "rrname": "185.194.93.14", "rdata": "circl.lu", "count": "19", "time_first": "16967
2{"rrtype": "AAAA", "rrname": "2a00:5980:93::14", "rdata": "circl.lu", "count": "18", "time_first":
3{"rrtype": "MX", "rrname": "10 cppy.circl.lu", "rdata": "circl.lu", "count": "149", "time_first": "
4{"rrtype": "NS", "rrname": "ns1.eurodns.com", "rdata": "circl.lu", "count": "5", "time_first": "169
5{"rrtype": "NS", "rrname": "ns2.eurodns.com", "rdata": "circl.lu", "count": "5", "time_first": "169
6{"rrtype": "NS", "rrname": "ns3.eurodns.com", "rdata": "circl.lu", "count": "5", "time_first": "169
7{"rrtype": "NS", "rrname": "ns4.eurodns.com", "rdata": "circl.lu", "count": "5", "time_first": "169
8{"rrtype": "SOA", "rrname": "ns1.eurodns.com hostmaster.eurodns.com 2023091306 43200 7200 1209600 8
```

`dribble-disable-active-query`

When the `dribble-disable-active-query` header is set, it is used to disable the active query resolver, which is enabled by default in CIRCL Passive DNS version 2. The value is discarded, as only the presence of the header is checked.

`dribble-filter-rrtype`

`dribble-filter-rrtype` is used to filter query on the Passive DNS for specific rrtype.

Example query

```
1curl -H 'dribble-filter-rrtype: SOA' https://www.circl.lu/pdns/query/circl.lu
```

```
1{"rrtype": "SOA", "rrname": "ns1.eurodns.com hostmaster.eurodns.com 2023091306 43200 7200 1209600 8
```

`dribble-paginate-count`

If a maxset error is return, the return set is limited to the maximum number of elements. To get all the values, pagination is required. The `dribble-paginate-count` set the number of element to return.

Example query

```
1curl -H 'dribble-paginate-count: 5' -H 'dribble-filter-rrtype: SOA' https://www.circl.lu/pdns/query
```

```
1
2{"rrtype": "SOA", "rrname": "a.gtld-servers.net nstld.verisign-grs.COM 1696809892 1800 900 604800 8
3{"rrtype": "SOA", "rrname": "a.gtld-servers.net nstld.verisign-grs.COM 1696811412 1800 900 604800 8
4{"rrtype": "SOA", "rrname": "a.gtld-servers.net nstld.verisign-grs.COM 1696816592 1800 900 604800 8
5{"rrtype": "SOA", "rrname": "a.gtld-servers.net nstld.verisign-grs.COM 1696818272 1800 900 604800 8
```

```
6{"rrtype": "SOA", "rrname": "a.gtld-servers.net nstld.verisign-grs.COM 1696820712 1800 900 604800 8
7
```

`dribble-paginate-cursor`

Example query

```
1curl -H 'dribble-paginate-count: 25' -H 'dribble-filter-rrtype: CNAME' -H 'dribble-paginate-cursor:
```

```
1HTTP/1.1 200 OK
2date: Sat, 21 Oct 2023 15:42:30 GMT
3content-type: application/x-ndjson
4server: dribble
5x-dribble-errors: []
6x-dribble-cursor: 7443482523371700254
7content-length: 4591
8
9{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.cthiinspectors.com", "count": "1", "
10{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.d1bproductions.com", "count": "2", "
11{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.dailystrange.com", "count": "1", "ti
12{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.davisdanceco.com", "count": "1", "ti
13{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.debarelli.com", "count": "1", "time_
14{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.depakhuys.com", "count": "1", "time_
15{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.dmr4u.com", "count": "1", "time_firs
16{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.dofbot.com", "count": "1", "time_fir
17{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.dpmonksfinance.com", "count": "1", "
18{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.dr-buba-best-traditional-healer.com"
19{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.dukecityriderz.com", "count": "1", "
20{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.eaglemedicinepsychicreadings.com", "
21{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.eroticescortdirectory.com", "count":
22{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.europeanfutsal.com", "count": "1", "
23{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.everythingbeautyskin.com", "count":
24{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.ewp-usa.com", "count": "1", "time_fi
25{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.fabricatorindia.com", "count": "1",
26{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.feelingsunfolding.com", "count": "1"
27{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.fineartfirm.com", "count": "1", "tim
28{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.fivestarluxurytravel.com", "count":
29{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.fpm-su.com", "count": "1", "time_firs
30{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.fultontransit.com", "count": "1", "t
31{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.futuramarge.com", "count": "1", "tim
32{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.higherground.ai", "count": "3", "tim
33{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "af.parkwayresort.ca", "count": "2", "ti
34
```

`x-dribble-cursor`

When pagination is enabled, the Passive DNS server returns the cursor for the next page, which can be set using `dribble-paginate-cursor`.

Error codes

Errors are returned in the `x-dribble-errors` header in JSON format.

maxset error type

The “maxset” error type indicates that the request is limited due to multiple existing records. This suggests the need to start paginating to retrieve the complete set of records.

```
x-dribble-errors: [{"error": "maxset", "record": "cdn1.wixdns.net", "value": 1000, "rrtype": "CNAME", "total_va
```

Example query and returned headers

```
curl -si https://www.circl.lu/pdns/query/cdn1.wixdns.net
```

```
HTTP/1.1 200 OK
date: Sat, 21 Oct 2023 16:03:14 GMT
content-type: application/x-ndjson
server: dribble
x-dribble-errors: [{"error": "maxset", "record": "cdn1.wixdns.net", "value": 1000, "rrtype": "CNAM
content-length: 151885

{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "2022photos.bostonkeygala.com", "count":
{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "aa.akasakachurch.com", "count": "3", "t
{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "aa.bayphoenixstudios.com", "count": "2"
{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "aa.canyonhillsptsa.com", "count": "1",
{"rrtype": "CNAME", "rrname": "cdn1.wixdns.net", "rdata": "aa.christinacollectionflooring.com", "c
```

Tools

Python Library to access the CIRCL Passive DNS API

We developed a Python library called PyPDNS to query any Passive DNS - Common Output Format.

Ruby Library to access the CIRCL Passive DNS API

PassiveDNS::Client is a rubygem developed by Chris Lee who includes access to different passive DNS services including CIRCL.

Scala library to access the CIRCL Passive DNS API

Scala library is a Scala implementation developed by Jason Jones.

R Library to access the CIRCL Passive DNS API

R Port of CIRCL.LU's PyPDNS Python module.

Go Language implementation to access the CIRCL Passive DNS API

Passive DNS client for CIRCL PDNS Database - golang implementation

C implementation to access the CIRCL and Farsight Security Passive DNS API

pure C implementation

Revision

- Version 1.0 - TLP:CLEAR - First version - 21st August 2014
- Version 2.0 - TLP:CLEAR - Second version - 2nd November 2023
