PDNS - API specification

Fyodor Yarochkin, V.B. Kropotov, Vitaly Chetvertakov

June 19, 2014

Contents

1 Revision History

1.1 Change Record

Version	Date	Name	Revision Description
2.1	*<2014-03-11 Wed>*	Fyodor	initial revision.

2 Introduction

PDNS is a system that indexes DNS queries data and performs some DNS-based detection/classification of DNS content.

This document describes API of the system.

3 Authentication

API is provided over HTTPs link at <pdns> url. Each system user should access system using API key which is passed to PDNS platform as additional HTTP POST or HTTP GET parameter.

4 Query API

PDNS platform allows to query different types of data. Following are the API endpoints that could be used to query variety of data collected by PDNS platform:

4.1 Query last detected domains/IPs

This query will return list of last domains, which were observed within last 60 seconds by DGA platform. Each domain entry will have source, DGA score, periodicity score and query response.

The each of the entry in this list has 60 second TTL, after which the entry will expire (and be deleted).

Each of the elements is deleted after query.

Query format:

```
POST /api/v1/lookup/last[/<query>]
    apikey=[apikey]

--optional--parameters
    callback_url=[url]
    score=<not less than score>
    ttl=<not older than ttl>
```

4.2 Query clusters

This query returns array of clusters and detected suspicious domain names.

```
POST /api/v1/lookup/clusters/[/<domain>]
    apikey=[apikey]

--optional--parameters
    callback_url=[url]
    score=<not less than score>
    ttl=<not older than ttl>
```

if query is specified, only clusters matching given <domain> name will be returned.

4.3 PDNS query

these queries support API similar to `https://api.dnsdb.info/`.

4.3.1 rrset queries

```
POST /api/v1/lookup/rrset/name/OWNER_NAME/<RRTYPE>/<BAILIWICK>/
    apikey=[apikey]

--optional--parameters
    callback_url=[url]
    score=<not less than score>
    ttl=<not older than ttl>
```

4.3.2 rdata queries

```
POST /api/v1/lookup/rdata/TYPE/VALUE/<RRTYPE>/
    apikey=[apikey]

--optional--parameters
    callback_url=[url]
    score=<not less than score>
    ttl=<not older than ttl>
```

5 Interpreting Results

Results are given in JSON format. TBD

6 Sample usage

```
#!/bin/sh
curl --insecure --data "api_key=key&score=0.2" https://pdnsmachine.org/api/v1/c
```