PUBLIC

ImmuniWeb’s Trademark Monitor API Documentation

Version v2.0

11th of April 2019

PUBLIC

Table of Contents

PUBLIC

General Overview

API Documentation and How-To

API Specifications

Field Name	Value
Protocol	HTTP/HTTPS
Request Type	GET
URL	https://www.immuniweb.com/radar/api/v1/scan/[ustamp].html- where "ustamp" is an arbitrary UNIX time-stamp (must be an integer). Such construction is done to prevent caching on client side.

POST Data Specifications

Field Name	Value
domain	the domain name to be tested.
limit	limit the amount of results shown.
offset	offset if results are limited
no_limit	0 or 1
	value of the token sent by the server if the tested domain is resolved into several IP addresses.
show_test_results	“true” will not show the result in the Recent Tests
recheck	"false" will use results from cache if the server has been tested within the past 24 hours, "true" will perform a new test without looking at the cache.

Example of Transaction Using CURL

 # New test (not cached)

$ curl -XPOST -d 'domain=twitter.com&dnsr=off&a=scan&recheck=false' 'https://www.immuniweb.com/radar/api/v1/scan/1451425590.html'

{"debug":true,"job_id":"2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc","status":"test_started","status_id":1,"message":"Test has started"}

 # You need to keep calling this until test is finished

$ curl -XPOST -d 'job_id=2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc' 'https://www.immuniweb.com/radar/api/v1/get_result/1451425590.html'

{"job_id":"2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc","status":"in_progress","status_id":2,"eta":2,"message":"Your test is in progress"}

 # New test (cached)

$ curl -XPOST -d 'domain=twitter.com&dnsr=off&a=scan&recheck=false'

'https://www.immuniweb.com/radar/api/v1/scan/1451425590.html'

{"test_id":"c84936eef26eeb8aaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb1004","status":"test_cached","status_id":3,"message":"Test is cached"}

$ curl -XPOST -d 'id=c84936eef26eeb8aaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb1004' 'https://www.immuniweb.com/radar/api/v1/get_result/1451425590.html'

 # Example with error

$ curl -XPOST -d 'domain=0.0.0.0&dnsr=off&a=scan&recheck=false' 'https://www.immuniweb.com/radar/api/v1/scan/1451425590.html'

{"error":"The domain name does not exist","error_id":9}

The output array will be composed of the following main elements that will be detailed later in this document:

• **meta-information**: containing basic meta-information, such as server info, geolocation, IP address, port, reverse DNS...

• **internals**: contains basic test information, such as title, description etc...

• **results**: containing all information about the test result, such as discovered typosquatting, cybersquatting and phishing domains discovered.

• **notifications**: contains high-level result descriptions.

Meta-information

Meta-information contains various information about the tested domain,

"server_ip":

- Syntax: string
- Always present
- Description: the IP address of the tested domain

"lat":

- Syntax: float
- Always present
- Description: the latitude of the IP address tested

"lng":

- Syntax: float
- Always present
- Description: the longitude of the IP address tested

"city":

- Syntax: string
- Always present
- Description: the city in which the tested server resides

"country":

• Syntax: string

• Always present

• Description: the country in which the IP address resides

"dnsr":

• Syntax: string

• Always present

• Description: do not show result

"total_phishing_urls_b1":

• Syntax: integer

• Always present

• Description: the number of phishing urls found

"total_phishing_urls_b2":

• Syntax: integer

• Always present

• Description: the number of typosquatting domains found

"total_phishing_urls_b4":

•Syntax: integer

• Always present

• Description: the number of cybersquatting domains found

"total_phishing_urls_b5":

• Syntax: integer

• Always present

• Description: the number of social network domains found

"total_phishing_urls_same_brand":

• Syntax: integer

• Always present

• Description: the total number of discovered phishing urls of the same brand

"total_phishing_urls":

• Syntax: { value: string, tag: integer }

• Always present

• Description: the total number of discovered phishing urls

"orig_url":

• Syntax: string

• Always present

• Description: the original url that was tested

"assesment_date":

• Syntax: float

• Always present

• Description: the date that the test has taken place on

"whois_registrar":

•Syntax: string

• Always present

• Description: the whois registrar of the tested domain

"whois_expiration_date":

• Syntax: integer

• Always present

• Description: the whois expiration date of the domain

"whois_creation_date":

• Syntax: integer

• Always present

• Description: the date of the whois entry for the domain

"whois_last_updated":

• Syntax: integer

• Always present

• Description: the last update of whois entry for the domain

"tld":

• Syntax: string

• Always present

• Description: the top-level domain

"total_runtime":

• Syntax: float

• Always present

• Description: the amount of time the test took to complete

Internals

contains basic test information, such as title, description and twitter title. The structure is as follows:

Syntax: {title: string, title_twitter: string, description: string, description_twitter: string}

Description: the values contain basic test information

"title":

• Syntax: string

• Always present

• Description: the title of the test, eg "Trademark Abuse Test of immuniweb.com"

"title_twitter":

- Syntax: string
- Always present
- Description: the title of the test that will appear on twitter

"description":

- Syntax: string
- Always present
- Description: an explanation of the radar test that is being carried out

"description_twitter":

- Syntax: string
- Always present
- Description: test statistics to be displayed on twitter

Results

This section is a list information about discovered domains, such as cybersquatting, typosquatting, phishing and social networks. The structure is as follows:

Syntax:

```
{
   phishing_block1: [
            ……
   ],
   phishing_block2 :[
      {
        ……
      }
   ], phishing_block3: [
                ……
    ],
```

```
  phishing_block4: [
     {
       ......
     }
  ], phishing_block5: [
                ......
  ],
  phishing_block5_total: [
                ......
  ]
}
```

Description: each phishing_block corresponds to an array that holds details on the different checks the radar service carry's out.

Phishing_block1

This list of values is part of 'results' and corresponds to found phishing domains.

"domain":

- Syntax: string
- Always present
- Description: the domain name of the phishing domain

"url":

- Syntax: string
- Always present
- Description: the url of the phishing domain

"ts":

- Syntax: float
- Always present
- Description: the timestamp of the test

"country":

• Syntax: string

• Always present

• Description: the domain name of the phishing domain

"tld":

• Syntax: string

• Always present

• Description: the top-level-domain of the phishing domain

" fuzzer":

• Syntax: string

• Always present

• Description: the fuzzer used for this check

"server_ip":

• Syntax: string

• Always present

• Description: the IP address of the phishing domain

"whois_registrar":

• Syntax: string

• Always present

• Description: the whois registrar of the phishing domain

"whois_expiration_date":

• Syntax: String

• Always present

• Description: the whois expiration date of the phishing domain

"whois_creation_date":

• Syntax: string

• Always present

• Description: the whois creation date of the phishing domain

"whois_last_updated":

• Syntax: string

• Always present

• Description: when the phishing domain was last updated in whois

"points":

• Syntax: integer

• Always present

• Description: the point score of the phishing domain

"is_email_server":

• Syntax: bool

• Always present

• Description: indicates if result is an email server

"is_web_server":

• Syntax: bool

• Always present

• Description: indicates if the result is a web server

Phishing_block2

This list of values is part of 'results' and corresponds to found typosquatting domains.

"domain":

• Syntax: string

• Always present

• Description: the domain name of the typosquatting domain

"url":

• Syntax: string

• Always present

• Description: the url of the typosquatting domain

"ts":

• Syntax: float

• Always present

• Description: the timestamp of the test

"country":

• Syntax: string

• Always present

• Description: the domain name of the typosquatting domain

"tld":

• Syntax: string

• Always present

• Description: the top-level-domain of the typosquatting domain

"fuzzer":

• Syntax: string

• Always present

• Description: the fuzzer used for this check

"server_ip":

• Syntax: string

• Always present

• Description: the IP address of the typosquatting domain

"whois_registrar":

• Syntax: string

• Always present

• Description: the whois registrar of the typosquatting domain

"whois_expiration_date":

• Syntax: String

• Always present

• Description: the whois expiration date of the typosquatting domain

"whois_creation_date":

• Syntax: string

• Always present

• Description: the whois creation date of the typosquatting domain

"whois_last_updated":

• Syntax: string

• Always present

• Description: when the typosquatting domain was last updated in whois

"points":

• Syntax: integer

• Always present

• Description: the point score of the typosquatting domain

"is_email_server":

• Syntax: bool

• Always present

• Description: indicates if result is an email server

"is_web_server":

• Syntax: bool

• Always present

• Description: indicates if the result is a web server

Phishing_block4

This list of values is part of 'results' and corresponds to found cybersquatting domains.

"domain":

• Syntax: string

• Always present

• Description: the domain name of the cybersquatting domain

"url":

• Syntax: string

• Always present

• Description: the url of the cybersquatting domain

"ts":

• Syntax: float

• Always present

• Description: the timestamp of the test

"country":

• Syntax: string

• Always present

• Description: the domain name of the cybersquatting domain

"tld:

• Syntax: string

• Always present

• Description: the top-level-domain of the cybersquatting domain

"fuzzer":

• Syntax: string

• Always present

• Description: the fuzzer used for this check

"server_ip:

• Syntax: string

• Always present

• Description: the IP address of the cybersquatting domain

" whois_registrar":

• Syntax: string

• Always present

• Description: the whois registrar of the cybersquatting domain

"whois_expiration_date":

• Syntax: string

• Always present

• Description: the whois expiration date of the cybersquatting domain

"whois_creation_date":

• Syntax: string

• Always present

• Description: the whois creation date of the cybersquatting domain

"whois_last_updated":

• Syntax: string

• Always present

• Description: when the cybersquatting domain was last updated in whois

"points":

- Syntax: integer
- Always present
- Description: the point score of the cybersquatting domain

"is_email_server":

- Syntax: bool
- Always present
- Description: indicates if result is an email server

" is_web_server":

- Syntax: bool
- Always present
- Description: indicates if the result is a web server

Phishing_block5

This list of values is part of 'results' and corresponds to found social network domains.

"domain":

- Syntax: string
- Always present
- Description: the domain name of the social network domain

"url:

- Syntax: string
- Always present
- Description: the url of the social network domain

" ts":

- Syntax: float
- Always present

• Description: the timestamp of the test

"country":

• Syntax: string

• Always present

• Description: the domain name of the social network domain

"tld:

• Syntax: string

• Always present

• Description: the top-level-domain of the social network domain

"fuzzer":

• Syntax: string

• Always present

• Description: the fuzzer used for this check

"server_ip:

• Syntax: string

• Always present

• Description: the IP address of the social network domain

"whois_registrar":

• Syntax: string

• Always present

• Description: the whois registrar of the social network domain

"whois_expiration_date":

• Syntax: string

• Always present

• Description: the whois expiration date of the social network domain

"whois_creation_date":

• Syntax: string

• Always present

• Description: the whois creation date of the social network domain

"whois_last_updated":

• Syntax: string

• Always present

• Description: when the social network domain was last updated in whois

"points":

• Syntax: integer

• Always present

• Description: the point score of the social network domain

"is_email_server":

• Syntax: bool

• Always present

• Description: indicates if result is an email server

"is_web_server":

• Syntax: bool

• Always present

• Description: indicates if the result is a web server

Notifications

Contains a textual description and overview of the test results, an integer will correspond to the relevant notifications for the test. The structure is as follows:

Syntax: [notification: integer, string]

"0":

• Syntax: string

• Always present

• Description: Domain example.com seems to be owned or operated by example

"1":

• Syntax: string

• Always present

• Description: In total we discovered $number websites that seem to be used to conduct cybersquatting and typosquatting attacks against tested domain name or brand.

"2":

• Syntax: string

• Always present

• Description: In total we discovered $number websites that seem to be used to conduct phishing attacks against tested domain name or brand.

Error handling

If an error occurs, only basic information and an error message will be returned the following way:

```
{ "error": string }

or

{ "error": string, "server_info": {
        "ip": string,
        "port": integer,
```

```
        "hostname": string,
        "reverse_dns": string
} }
```

Possible error messages which system can return are:

error	Test doesn't exist.
error	API key is not valid. Please double check it.
error	You have performed N tests in last 3 minutes. The system is currently busy, please try again later.
error	You have performed N tests in the last 24 hours. The system is currently busy, please try again later.
error	System is very busy now, please try again later.
error	You reached the limit of N total running tests. Wait for one to finish, than retry.
error	The domain name cannot be resolved.
error	The domain name does not exist.
error	An error has occured while checking DNS records of domain.
error	Error: the resolved IP does not belong to an allowed range.
error	Only domain names are allowed in queries.
error	URL points to non-html content.
error	Could not connect to server.

Appendix 1: List of Messages values

ID	Value
1	The web server is not currently accessible, test results may be incomplete or inaccurate.
2	Domain #DOMAIN# seems to be owned or operated by #OWNER#.
3	The web server points to non-html content, test results may be incomplete or inaccurate.

Appendix 3: List of Descriptions values

ID	Value
1	the IP address tested
2	the latitude of the IP address tested
3	the longitude of the IP address tested
4	the city in which the IP address reside
5	the country in which the IP address resides
6	Do not show result
7	the number of phishing urls found
8	the number of typosquatting domains found
9	the number of cybersquatting domains found
10	the number of social network domains found
11	the total number of discovered phishing urls of the same brand
12	the total number of discovered phishing urls
13	the original url that was tested
14	the date that the test has taken place on
15	the whois registrar of the tested domain
16	the whois expiration date of the domain
17	the date of the whois entry for the domain
18	the last update of whois entry for the domain
19	the top-level domain
20	the amount of time the test took to complete
21	the title of the test, eg "Trademark Abuse Test of immuniweb.com"
22	the title of the test that will appear on twitter
23	an explanation of the radar test that is being carried out
24	test statistics to be displayed on twitter
25	test statistics to be displayed on twitter
26	the domain name of the phishing domain
27	the url of the phishing domain
28	The timestamp of the test
29	the domain name of the phishing domain
30	an explanation of the radar test that is being carried out
31	the fuzzer used for this check
32	the IP address of the phishing domain
33	the whois registrar of the phishing domain
34	the whois expiration date of the phishing domain
35	the whois creation date of the phishing domain
36	when the phishing domain was last updated in whois
37	the point score of the phishing domain
38	indicates if result is an email server
39	indicates if the result is a web server
40	the domain name of the typosquatting domain
41	the url of the typosquatting domain
42	The timestamp of the test
43	the domain name of the typosquatting domain
44	an explanation of the radar test that is being carried out

45	the fuzzer used for this check
46	the IP address of the typosquatting domain
47	the whois registrar of the typosquatting domain
48	the whois expiration date of the typosquatting domain
49	the whois creation date of the typosquatting domain
50	when the typosquatting domain was last updated in whois
51	the point score of the typosquatting domain
52	indicates if the result is an email server
53	indicates if the result is a web server
54	the domain name of the cybersquatting domain
55	the url of the cybersquatting domain
56	The timestamp of the test
57	the domain name of the cybersquatting domain
58	an explanation of the radar test that is being carried out
59	the fuzzer used for this check
60	the IP address of the cybersquatting domain
61	the whois registrar of the cybersquatting domain
62	the whois expiration date of the cybersquatting domain
63	the whois creation date of the cybersquatting domain
64	when the cybersquatting domain was last updated in whois
65	the point score of the cybersquatting domain
66	indicates if the result is an email server
67	indicates if the result in a web server
68	the domain name of the social network domain
69	the url of the social network domain
70	The timestamp of the test
71	the domain name of the social network domain
72	an explanation of the radar test that is being carried out
73	the fuzzer used for this check
74	the IP address of the social network domain
75	the whois registrar of the social network domain
76	the whois expiration date of the social network domain
77	the whois creation date of the social network domain
78	when the social network domain was last updated in whois
79	the point score of the social network domain
80	indicates if the result is an email server
81	indicates if the result is a web server

Appendix 4: List of Highlights values

ID	Value
1	There are #TOTAL_MALICIOUS# malicious websites for all domains (in different TLDs) of #BRAND#
2	In total we discovered #TOTAL websites that seem to be used to conduct #NAME attacks against tested domain name or brand.

3	Domain #DOMAIN# seems to be owned or operated by #OWNER#
4	Currently we are not aware of any cybersquatting, typosquatting, phishing domains for #URL domain.

Appendix 5: List of Error messages

error_id	error
1	You have performed N tests in the last 3 minutes. The system is currently busy, please try again a bit later.
2	You have performed N tests in the last 24 hours. The system is currently busy, please try again a bit later.
3	Sorry, our systems are very busy now, we are working on the issue. Please try again in a few minutes.
4	You reached the limit of N concurring running tests. Please wait until at least one of them is finished.
5	Sorry, your API key is invalid or has expired. Please double-check it or contact us.
7	The domain name cannot be resolved
9	The domain name does not exist
10	An error has occured while checking DNS records of domain
13	We could not conduct the requested test because a timeout occurred.
14	Arbitrary error from engine.
17	An error occurred while encoding results.
18	Test does not exist.
19	Too many downloads of PDF.
20	Not logged in.
21	Too many downloads of HTML.