DARK WEB EXPOSURE TEST

API Documentation v 2.3.2

February 28, 2022

Table of Contents

1. General Overview

API Documentation and How-To

API Specifications

Field Name	Value
Protocol	HTTP/HTTPS
Request Type	POST
URLs	To initiate the test: https://www.immuniweb.com/darkweb/api/v1/scan/[ustamp].html To fetch the results: https://www.immuniweb.com/darkweb/api/v1/get_result/[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.
dnsr	"on" means that test results will be hidden, "off" means that test results will be displayed in the statistics on ImmuniWeb.com.
recheck	"false" will use results from cache if the domain has been tested within the past 24 hours, "true" will perform a new test without looking at the cache.
limit	Limit the amount of results shown.
offset	Offset if results are limited
no_limit	0 or 1
a	“a” stands for action. Example: “a=scan”
api_key	Secret token which you submit alongside with the request (used only for commercial access)

Example of Transactions Using CURL

Step 1: Starting the test

curl -d “domain=twitter.com&dnsr=off&a=scan&recheck=false&choosen_ip=any”
https://www.immuniweb.com/darkweb/api/v1/scan/1451425590.html

If you receive the “test_cached” status in response, please proceed to Step 2.b

If you receive the “test_started” status in response, please proceed to Step 2.a

Response Example (if the test has been found in the cache)


```
{
  "test_id": "c84936eef26eebaef5ffc43f38ddb91adfd90ac27fb416bd0b21fe2edb1004",
  "status": "test_cached",
  "status_id": 3,
  "message": "Test is cached"
}
```


Response Example (if the test has **not** been found in the cache):


```
{
  "debug": true,
  "job_id": "2a9e1f1bc9dc0c7a4bde930dff488771eea6d36988208d34163c5496227b8dc",
  "status": "test_started",
  "status_id": 1,
  "message": "Test has started"
}
```


Step 2.a: Fetching the results if the test was not found in the cache (call this until the test is finished)

curl -d “job_id=[job_id FROM STEP 1 RESPONSE]”
https://www.immuniweb.com/darkweb/api/v1/get_result/1451425590.html

Response Example (if the test is **not** finished yet):


```
{ "job_id": "2a9e1f1bc92dc0c7a4bde930dff488771eea6d36988208d34163c549622b8dc",
  "status": "in_progress",
  "status_id": 2,
  "message": "Your test is in progress" }
```

Step 2.b: Fetching the results if the test was found in the cache (“test_cached” status)

curl -d “id=[test_id FROM THE STEP 1 RESPONSE]”
https://www.immuniweb.com/darkweb/api/v1/get_result/1451425590.html

Example with error

curl -d “domain=0.0.0.0&dnsr=off&a=scan&recheck=false”
https://www.immuniweb.com/darkweb/api/v1/scan/1451425590.html

Error Response Example

```
{
  "error": "string", "error_id": "integer"
}
```

How to download the PDF report

curl -d “api_key=YOUR-API-KEY”
“https://www.immuniweb.com/darkweb/gen_pdf/[test_id]” > report.pdf

The returned response of a successful test will be composed of the following main elements that will be detailed later in these sections of the document:

- Meta-information: containing basic meta-information, such as server info, geolocation, IP address, port, reverse DNS, etc.
- Internals: contains basic test information, such as title, description, etc.
- Results: contains all information about the test result, such as discovered typosquatting, cybersquatting and phishing domains.
- Notifications: contains high-level result descriptions.

Successful Response Example


```
{
  "server_ip": "172.217.13.110",
  "lng": -80.135000000000005,
  "lat": 26.937000000000001,
  "city": "Jupiter",
  "company_name": "Google LLC",
  "tld": ".com",
  "has_freemail": false,
  "whois_registrar": "MarkMonitor Inc.",
  "whois_creation_date": 874274400,
  "whois_last_updated": 1567980000,
  "whois_expiration_date": 1852495200,
  "owned_by": "Google LLC",
  "orig_url": "google.com",
  "assesment_date": 1582158086.760741,
  "total_runtime": 238.60002708435059,
  "country": "United States",
  "id": "8e3fca7d25532f44b7af5e4858474754209fb644aab825f1494684b3d7936f59",
  "short_id": "3dAMXgrD",
  "dnsr": "on",
  "total_phishing_urls": 1815,
  "total_phishing_urls_b2": 112,
  "total_phishing_urls_b4": 1262,
  "total_phishing_urls_b5": 91,
  "legitimate_phishing_urls_b2": 32,
  "legitimate_phishing_urls_b5": 0,
  "legitimate_phishing_urls_b4": 289,
  "malicious_phishing_urls_b2": 80,
  "malicious_phishing_urls_b4": 973,
  "malicious_phishing_urls_b5": 91,
  "favicon": "d4c9d9027326271a89ce51fcafed673f17be33469ff979e8ab8dd501e664f",
  "is_cutted": false,
  "cutted_router": "user_not_logged_in",
  "internals": {},
  "results": {},
  "notifications": []
}
```

2. Meta-information

Field Name	Type	Always present	Description
server_ip	string	Yes	The IP address of the tested domain.
lat	float	Yes	The latitude of the IP address tested.
lng	float	Yes	The longitude of the IP address tested.
city	string	Yes	The city in which the tested server resides.
country	string	Yes	The country in which the IP address resides.
dnsr	string	Yes	Do not show results on ImmuniWeb.com.
company_name	string	Yes	The company's name.
tld	string	Yes	The top-level domain.
has_freemail	bool	Yes	Indicates if the domain has a free mail service.
orig_url	string	Yes	The original URL that was tested.
assesment_date	float	Yes	The date that the test has taken place on.
total_runtime	float	Yes	The amount of time the test took to complete.
id	string	Yes	The id of the test.
short_id	string	Yes	The short id of the test.
whois_registrar	string	Yes	The whois registrar of the tested domain.
whois_creation_date	integer	Yes	The date of the whois entry for the domain.
whois_last_updated	integer	Yes	The last update of whois entry for the domain.
whois_expiration_date	integer	Yes	The whois expiration date of the domain.
total_phishing_urls	integer	Yes	The total number of discovered phishing URLs.
total_phishing_urls_b1	Deprecated		
total_phishing_urls_b2	integer	Yes	The number of typosquatting domains found.
total_phishing_urls_b4	integer	Yes	The number of cybersquatting domains found.

total_phishing_urls_b5	integer	Yes	The number of social network domains found.
total_phishing_urls_same_brand	integer	Yes	The total number of discovered phishing urls of the same brand.
legitimate_phishing_urls_b2	integer	Yes	The number of discovered URLs in the block 2 that appear to be legitimate.
legitimate_phishing_urls_b4	integer	Yes	The number of discovered URLs in the block 4 that appear to be legitimate.
legitimate_phishing_urls_b5	integer	Yes	The number of discovered URLs in the block 5 that appear to be legitimate.
malicious_phishing_urls_b1	Deprecated		
malicious_phishing_urls_b2	integer	Yes	The number of discovered potentially malicious URLs in block 2.
malicious_phishing_urls_b4	integer	Yes	The number of discovered potentially malicious URLs in block 4.
malicious_phishing_urls_b5	integer	Yes	The number of discovered potentially malicious URLs in block 5.
favicon	bool	Yes	Indicates the presence of favicon.
is_cutted	bool	Yes	“true” if not all results are shown.
cutted_router	string	Yes	Describes the action to make the hidden results visible.
darkweb_stats	object	Yes	Contains information on Dark Web exposure: number of total and verified incidents, their estimated risk level, and the classification of the verified indicents.
phishing_stats	object	Yes	Contains information on the total number of discovered phishing URLs and their risk level.
internals	object	Yes	Contains basic test information, such as title, description, etc. Will be detailed later in the document.
results	object	Yes	Contains information about typosquatting, cybersquatting and phishing domains. Will be detailed later in the document.
notifications	array	Yes	Contains high-level result descriptions. Will be detailed later in the document.

3. Internals

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

Field Name	Type	Always present	Description
id	string	Yes	The short id of the test
title	string	Yes	The title of the test (e.g. "Trademark Abuse Test of immuniweb.com")
title_twitter	string	Yes	The title of the test that will appear on twitter.
description	string	Yes	An explanation of the darkweb test that is being carried out.
description_twitter	string	Yes	Test statistics to be displayed on twitter.
can_index	bool	Yes	Indicates if the test can be indexed.
scores	object	Yes	Contains summary information regarding the number of Dark Web, phishing, cybersquatting, typosquatting and social network related issues found.

4. Results

This section contains information about discovered cybersquatting, typosquatting, phishing and social network domains. The structure is as follows:

```
"results": {
  "phishing": […],
  "phishing_block1": DEPRECATED,
  "phishing_block2": […],
  "phishing_block4": […],
  "phishing_block5": […],
}
```

Description: each section will be detailed later in the document.

Phishing

Each object in this array has the following structure:

```
        "hostname": "string",
        "urls": []
```

The “urls” array contains details on the potential phishing webpages.

Field Name	Type	Always present	Description
risk	string	Yes	Indicates how similar is the phishing webpage to the legitimate one.
screenshot	string	Yes	Contains the hash of the screenshot of the phishing webpage.
url	string	Yes	Indicates the URL of the phishing webpage.
country	string	Yes	Indicates the location of the server.
created_at	integer	Yes	Indicates the creation date.
hostname	string	Yes	Indicates the hostname.
resolved_ip	string	Yes	Indicates the server’s IP address.
content	string	Yes	Contains the hash of the HTML source of the phishing webpage.
score	integer	Yes	Indicates the calculated score of the phishing webpage.
whois	object	Yes	Contains the whois information of the domain.

The structure of the “whois” object is as follows:

Field Name	Type	Always present	Description
registrar	string	Yes	Indicates the registrar of the domain.
registrant	string	Yes	Indicates the registrant.
creation	integer	Yes	Indicates the domain’s creation date.
last_updated	integer	Yes	Indicates the domain’s last update date.
expiration	integer	Yes	Indicates the domain’s expiry date.

Phishing_block2

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

Field Name	Type	Always present	Description
status	string	Yes	The status of the typosquatting domain .
domain	string	Yes	The domain name of the typosquatting domain.
whois_registrar	string	Yes	The whois registrar of the typosquatting domain.
server_ip	string	Yes	The IP address of the typosquatting domain.
url	string	Yes	The URL of the typosquatting domain.
country	string	Yes	The country in which the typosquatting domain resides.
ts	float	Yes	The timestamp of the test.
is_email_server	bool	Yes	Indicates if result is an email server.
Is_web_server	bool	Yes	Indicates if the result is a web server.
whois_creation_date	integer	Yes	The date of the whois entry for the typosquatting domain.
whois_last_updated	integer	Yes	The last update of whois entry for the typosquatting domain.
whois_expiration_ date	integer	Yes	The whois expiration date of the typosquatting domain.
tld	string	Yes	The top-level-domain of the typosquatting domain.
fuzzer	string	Yes	The fuzzer used for this check.
id	string	Yes	The id of the typosquatting domain.
legitimate	bool	Yes	Indicates if the URL is legitimate.

Phishing_block4

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

Field Name	Type	Always present	Description
status	string	Yes	The status of the cybersquatting domain.
domain	string	Yes	The domain name of the cybersquatting domain.
whois_registrar	string	Yes	The whois registrar of the cybersquatting domain.
server_ip	string	Yes	The IP address of the cybersquatting domain.
url	string	Yes	The url of the cybersquatting domain.
country	string	Yes	The country in which the cybersquatting domain resides.
ts	float	Yes	The timestamp of the test.
is_email_server	bool	Yes	Indicates if result is an email server.
Is_web_server	bool	Yes	Indicates if the result is a web server.
whois_creation_date	integer	Yes	The date of the whois entry for the cybersquatting domain.
whois_last_updated	integer	Yes	The last update of whois entry for the cybersquatting domain.
whois_expiration_ date	integer	Yes	The whois expiration date of the cybersquatting domain.
tld	string	Yes	The top-level-domain of the cybersquatting domain.
fuzzer	string	Yes	The fuzzer used for this check.
id	string	Yes	The id of the cybersquatting domain.
legitimate	bool	Yes	Indicates if the URL is legitimate.

Phishing_block5

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

Field Name	Type	Always present	Description
domain	string	Yes	The domain of the social network.
whois_registrar	string	Yes	The whois registrar of the social network domain.
network	string	Yes	The name of the social network.
server_ip	string	Yes	The IP address of the social network domain.
url	string	Yes	The url of the social network domain.
country	string	Yes	The country in which the social network domain resides.
brand	string	Yes	The brandname of the network.
ts	float	Yes	The timestamp of the test.
is_email_server	bool	Yes	Indicates if result is an email server.
Is_web_server	bool	Yes	Indicates if the result is a web server.
whois_creation_date	integer	Yes	The date of the whois entry for the social network domain.
whois_last_updated	integer	Yes	The last update of whois entry for the social network domain.
whois_expiration_date	integer	Yes	The whois expiration date of the social network domain.
tld	string	Yes	The top-level-domain of the social network domain.
fuzzer	string	Yes	The fuzzer used for this check.
id	string	Yes	The id of the social network domain.
legitimate	bool	Yes	Indicates if the URL is legitimate.

5. 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:

	Always present	Value
1	No	In total we discovered **$number** of websites that seem to be used to conduct cybersquatting and typosquatting attacks against tested domain name or brand.
2	No	In total we discovered **$number** websites that seem to be used to conduct phishing attacks against tested domain name or brand.
3	No	Currently we are not aware of any cybersquatting, typosquatting, phishing domains for #URL domain.
4	No	Domain example.com seems to be owned or operated by **example.co**

Appendix 1: List of Message 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 2: List of Error messages

error_id	error
0	Unknown error. Please contact us.
1	You have performed [N] [ACTIONS] in the last 3 minutes. Please try again a bit later.
2	You have performed [N] [ACTIONS] in the last 24 hours. Buy premium API to run more tests.
3	Sorry, our systems are very busy now. Please try again in a few minutes.
4	You have running [N] concurrent [ACTIONS]. Please try again a bit later.
5	Sorry, there is a problem with your API key. Please double-check it or contact us.
6	Test is forbidden. Please contact us.
7	The domain name cannot be resolved. Please double-check it or contact us.
9	The domain name does not exist. Please double-check it or contact us.
10	An error has occured while checking DNS records of domain. Please double-check it or contact us.
11	Invalid IP address. Please double-check
12	Error with token. Our API has changed, please double-check it or contact us.
13	We could not conduct the requested test because a timeout occurred.
14	Arbitrary error from the engine.
16	Domain name was resolved in an invalid IP address.
17	An error occurred while encoding results.
18	Test does not exist.
19	PDF rendering problem has occurred.
20	Please register to [PERFORM_ACTION]
21	Your API key has exceeded the action-per-time limits. Please wait or contact us to increase the limits.
22	Your API key has expired. Please contact us to get a new one.
23	Your API key has been issued for another service.
24	Your API key does not exist.
25	Access denied for [IP_ADDRESS].
29	Only domain names are allowed.