WMC GLOBAL

WORLDWIDE BRAND AND CUSTOMER PROTECTION AT SCALE

PHISHFEED
API DOCUMENTATION

V2.1 08.08.2024

WMC GLOBAL

TABLE OF CONTENTS

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

GETTING STARTED WITH PHISHFEED

The PhishFeed API is a transparent threat intelligence tool for querying known phishing URLs. Query by any brand, URL, geolocation, or IP and grab the intelligence that's needed. Pull the data whenever and however: Run it once a minute, once a day, or once a week. Response data can populate security orchestration, automation, and response (SOAR) and security information and event management (SIEMs) with known indicators of compromise (IOCs) for blocking known threats. The data is also essential for threat analysts trying to identify brand and industry attack trends, hosting location, identified phishing kits, and if an attack was mobile-focused. With PhishFeed you can:

- Scan millions of URLs and identify thousands of phishing URLs per day
- View URL, impersonated brand, IP, ASN Data, hosted geo-location, mobile attack, threat actor email (when available), and phishing kit name provided (when available). Over 700 brands are identified, available, and growing.
- Full access to the PhishFeed data feeds details all phishing attacks allowing customers to monitor both your brand and industry attacks at a high level.
- Gain full visibility into the phishing attack landscape to better position your organization to deal with your specific threats
- Drive takedowns and enforcement

DOCUMENT STATUS

This document supports v2.1 for the WMC Global PhishFeed API. The API and documentation are subject to change.

[WMC Global Website]

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

WMC GLOBAL

PHISHFEED DATA DICTIONARIES

DATA DICTIONARY SEARCH PARAMETERS

PARAMETER NAME	DESCRIPTION	DATA TYPE
order	ASC or DESC Order of the URLs returned, determined by the discovery time.	string
brand	A searchable substring found in the associated brand. **EXAMPLE:** Entering face returns all URLs associated with the brand "facebook" and any other URLs with face in the brand parameter.	string
days	Retrieve data this many days prior. **EXAMPLE:** Entering 5 returns data from the past five days.	integer
hours	Retrieve data this many hours prior. **EXAMPLE:** Entering 5 returns data from the past five hours.	integer
minutes	Retrieve data this many minutes prior. **EXAMPLE:** Entering 5 returns data from the past five minutes.	integer
url_term	A searchable substring in the URL. Can utilize wildcard searches **EXAMPLE:** *PayPal* would return results with "PayPal" in the url parameter.	string
urls	The count of URLs to return. A default of 10,000 URLs are returned. A maximum 20,000 can be returned. **EXAMPLE:** A blank entry would return up to 10,000 URLs.	string
ip	A searchable substring found in the IP address of the hosted phishing page. **EXAMPLE:** Entering 32.54.6 returns all data with “32.54.6” in the ip field	string
country	The name of the hosted IP address's country. **EXAMPLE:** Entering bulg would return all URLs hosted in	string

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

	Bulgaria in the ip_location.	
country_code	The specified ISO country code for the country of the IP address. **EXAMPLE:** Entering DE returns all URLs hosted in Germany in the ip location	string
city	The name of the city where the IP is hosted. **EXAMPLE:** Entering Wash returns all URLs hosted in Washington in the ip_location	string
region	The name of the region where the server of the IP is hosted **EXAMPLE:** Entering Del returns all URLs hosted in Delaware in the ip_location	string

DATA DICTIONARY OUTPUT PARAMETERS

PARAMETER NAME	DESCRIPTION	DATA TYPE
count	The total URLs returned	integer
data	A list of phishing URLs and related metadata Including id, url, ip, ip_location, ip_as, ip_asn, date_found, brand, zip_emails, zip_kits.	array of dictionaries
id	The unique PhishFeed URL identifier.	integer
url	The returned confirmed phishing URL.	string
ip	The IP address of the hosted phishing page.	string
ip_location	The IP address location (country_code, region, city) of the hosted phishing page.	string
ip_as	The IP address autonomous system number.	string
ip_asn	The IP address autonomous system name.	string
date_found	The UTC date and time the phishing URL was discovered.	string

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

brand	The brand that is being impersonated by the phishing page.	string
zip_kits	(If available) The name of up to 1 phishing kit found related to the phishing URL.	string
zip_emails	(If available) Up to 2 email addresses of threat actors identified in the associated phishing kits.	string
mobile	Identifies if the phishing URL is confirmed as a mobile attack.	boolean

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

PHISHFEED RESPONSES

BASE URL: api.phishfeed.com/v2

SCHEME: HTTPS

API: GET /feed

CONTENT TYPE: application/JSON

RESPONSE SIZE LIMIT

The API returns is limited to 6MB of data up the nearest entire record per request.

RESPONSE CODE	DESCRIPT ION
200	Success

JSON


```
{
  "count": 1,
  "data": [
    {
      "id": "1042603",
      "url": "https://www.acuo.com.br/",
      "ip": "3.88.234.39",
      "ip_location": "US, Virginia, Ashburn",
      "ip_as": "AS14618",
      "ip_asn": "AMAZON-AES, US",
      "date_found": "2020-04-22 14:30:05",
      "brand": "WhatsApp",
      "zip_kits": "login-Authentication.zip",
      "zip_emails": "hughesernest2@gmail.com"
      "mobile": true
    }
  ]
}
```


© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

WMC GLOBAL

PHISHFEED FAQ

What can I do to improve the number of phish, credentials, and phishing kits collected by WMC Global solutions?

For organizations with PhishFeed, Compromised Credential Recovery, and KITIntel, the best place to leverage threat information in within an organization's own data.

- **WEBSITE REFER LOGS** - Many phishing sites redirect to legitimate websites. Sending referrer URLs to the URL Submission API improves our ability to identify phish that are impersonating the client's brand and attacking their customers.
- **REPORTED ABUSE BOX URLS** - By submitting URLs from complaints to the URL Submission API WMC Global services can help an organization quickly identify phishing that is targeting their employees and customers so they can take action.

What is the Unique ID in the API used for?

The `id` represents a specific URL in the database and can help when troubleshooting, especially for:

- Multiple URLs from the same domain came in during a similar time period
- Different systems can have odd interactions when encoding, Punycode, and Unicode. Issues may even occur when copying and pasting
- There are many techniques that threat actors use to make URLs look similar to legitimate organization domains, specifically to confuse human eyes. The ID can help the user troubleshoot why there might be differences in responses.
- Two URLs have very similar characters. and the reader may read them as the same URL `www.banking.boa.uk.com` vs `www.bonking.boa.uk.com`.

How far back in the PhishFeed API can I query?

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute

PhishFeed can query up to 30 days into the past and return up to up to 6MB of data up to the nearest entire record per request.

Do all PhishFeed URLs have a brand associated with them?

No. Some URLs are marked as “undetermined”. WMC Global is constantly adding new brands to our collection.

Do all Phishing URLs have every brand associated with them?

No. PhishFeed identifies the most prominent brand associated with a phish to include.

How do I query for partial URLs?

The field `url_term` accepts wildcards as `*`

EXAMPLE: `*bank*`

Sample Curl

cURL

```
curl -X 'GET' \
  'https://api.phishfeed.com/v2/feed?url_term=*ban
  k*' \
  -H 'accept: application/json' \
  -H 'x-api-key: [ENTER YOUR KEY]'
```

© 2024 WMC Global Proprietary and Confidential | Do Not Distribute