

# Domain & IP Threat Intelligence API

Speed up threat investigations and add more coverage to your security products with:

- Fresh threat ratings
- Real-time verdicts
- Content categorization
- Impersonation probability
- Geolocation
- Popularity
- Language
- ...and more

```
curl -H 'Content-Type: application/json'
-d '{"uri":"risky.site","license":"key",
"type":"partner.info","version":1}'
https://api.alphamountain.ai/threat/uri/

{
  "status": {
    "threat": "Success"
  }
  "threat": {
    "scope": 7,
    "scope": "domain",
  },
  "ttl":28800
}
```

## Partners

alphaMountain is integrated with leading threat management platforms.

  
MALTEGO VIRUSTOTAL  
splunk> CYWARE™  
SECURE X

### MALICIOUS RISK

0-10 scale or reputation



### THREAT FACTORS

Indicators contributing to risk



### CONTENT CATEGORIZATION

83 content categories



### IMPERSONATION RISK

Cybersquatters, phishing detection



### ADDITIONAL CONTEXT

Popularity, language & WHOIS



**START YOUR FREE TRIAL**

api@alphamountain.ai



# threatYeti: Domain Research Platform

Visualize the risk of any host, domain, or IP address with a comprehensive, real-time security analysis including:

## RISK RATING

## THREAT FACTORS

## CATEGORIES

## RELATED HOSTS

**0u6cx7n.vxbgrgs.cn** Risk **8.76** 

**Summary**

Risk Rating: Low Warning High

Factors: 1 Low Risk 3 Warning 4 High Risk

Categories: Malicious, Phishing

Popularity Rank: > 5,000,000

Whois Date Created: 2022-05-09 (10 months ago)

Certificate: Unavailable

IP Networks:  103.224.182.210 (Trellian Pty. Limited)

Hosts on IP: 5000+ (2,000+ risky)

Root Domain: 9.25  vxbgrgs.cn

**RELATED HOSTS**


Relationship	Total	Risky
Shared IP	5000+	2,000+
Same Domain	69	57
Inbound Redirects	0	0
Outbound Redirects	0	0
Inbound Links	0	0
Outbound Links	0	0
Certificate Altnames	0	0

**FACTORS**

Show **10** entries


Hostname	Risk Rating
0.0ca.npool.pw	5.22
000p.live	4.75
003fvo.link	5.18
00b.live	4.22
00u.live	4.33
01091991949.com	4.75
02ma.xyz	9.21
0358e.0373p.cn	9.23
04ngxgo.sxtoddandrew.cn	9.31
06238888.xyz	5.00

Showing 1 to 10 of 5,000 entries


Date Captured   
2023-03-15 (today)


IPv4  103.224.182.210 (133618 Trellian Pty. Limited)


Addresses

IPv6  <none>

Addresses

Reverse Lookup  
3.12  lb-182-210.above.com

Name Servers  
ns1.abovedomains.com  
AU  103.224.182.5 (Trellian Pty. Limited)  
ns2.abovedomains.com  
AU  103.224.182.6 (Trellian Pty. Limited)

Mail Servers  
park-mx.above.com  
AU  103.224.212.34 (Trellian Pty. Limited)

Specialty IP  
Unavailable

DKIM  
df67490d49f24b046be96d96a13e7022af781ed6  
v=spf1 -all

SPF  
v=spf1 -all

TXT  
v=spf1 -all  
df67490d49f24b046be96d96a13e7022af781ed6

## PASSIVE DNS

## RESPONSES

### HTTP

Status  
**200**

### Redirect Chain

http://0u6cx7n.vxbgrgs.cn [301] ↓  
http://ww16.0u6cx7n.vxbgrgs.cn/?  
sub1=20230308-1134-16cc-93e2-f2fc1a547944  
[200]

### Headers

```
{
  date: "Wed, 08 Mar 2023 00:34:17 GMT",
  vary: "Accept-Encoding",
  pragma: "no-cache",
  server: "NginX",
  expires: "Mon, 26 Jul 1997 05:00:00 GMT",
  connection: "close",
  content-type: "text/html; charset=UTF-8",
  x-powered-by: "PHP/8.1.9",
  cache-control: "no-store, no-cache, must-revalidate, post-check=0, pre-check=0";
}
```

## AND MORE...



BE THE APEX PREDATOR OF EVERY HUNT

threatYeti.com

