User Guide

# DomainTools Hosting IP Risk Feed

DOMAINTOOLS®

# Hosting IP Risk Feed

DomainTools' list of all active domain-linked IPs delivers organizations the entire risk spectrum for available domain hosting IPs.

## Find Threats Before They Find You

Existing IP reputation feeds have important limitations in both accuracy and coverage. Many IP addresses host domains registered with malicious intent but have not yet been observed on industry blocklists. These IP addresses may represent a risk to the organization but a blind spot in traditional IP-based defenses or intelligence sources. Unlike traditional IP reputation lists, the DomainTools Hosting IP Risk Feed reflects the fine-grained, predictive assessments of the popular DomainTools Domain Risk Score for any domains hosted on an IP. Because the Domain Risk Score reliably predicts how likely a given domain is to be malicious, even before the domain has been weaponized, an aggregate Risk Score of all domains on a given IP address provides a high-confidence view of the risk level of the IP.

---

# Hosting IP Risk Feed Description

Hosting IP Risk Feed is a comprehensive list of IPs, with all available IP hosting domains from high to low risk. For each IP, the Hosting IP Risk Feed displays IPV4 and Domain Risk Score percentages (Phishing, Malware, Spam, and Proximity) and data from deterministic threat intel feeds in addition to verifying that the IP is "active" based on observations of pDNS traffic. The list is generated daily, providing the most current scores for active domains each day.

## Hosting IP Risk Feed Components

The risk assessment component of IP Hotlist is enabled by a combination of Domain Risk Score & several highly curated threat intel feeds.  Drawing upon data points from more than 330 million current Internet domains, Domain Risk Score predicts how likely a domain is to be malicious, often before it is weaponized that predictive power is now available for IP Hotlist. The malicious domain percentages come from two distinct algorithms and numerous threat intel feeds:

1. Proximity evaluates the likelihood a domain may be part of an attack campaign by analyzing how closely connected it is to other known-bad domains.
2. Threat Profile leverages machine learning to model how closely the domain's intrinsic properties resemble others used for spam, phishing, or malware. The strongest signal from either of those algorithms becomes the combined Domain Risk Score.
3. DomainTools partners with numerous third-party threat intel feed which provide known malicious domains as they are convicted on a daily basis. This is combined with DomainTools predictive scoring to determine the percentage of known and predicted malicious domains in an IP.

## Hosting IP Risk Feed Contents

In summary, Hosting IP Risk Feed will conform to the following requirements:

- The Hosting IP Risk Feed will publish once daily
- Hosting IP Risk Feed contains IPs that are
    - Associated with pDNS activity one day ago
    - Have domains pointed to them in the last 24 hours
    - All risk percentages (IPs with 0 malicious domains as well as IPs with only malicious domains)
- IPs with "Zero-listed" also known as manually curated benign domains will be known in the Hosting IP Risk Feed with a specific field
- The list will be variable in size based on the domains that fit the criteria each day
    - Size cannot be guaranteed or bounded. Current expectations are that the list is between 15.5M and 20M entries.
    - Domains pointing to the IP will be rescored each day and placed on the list

Hosting IP Risk Feed will be available in a tab-separated CSV file, containing the following columns in the order displayed below:

| Field Name | Field Description |
|---|---|
| ip | IP with www/apex domains pointing to it |
| pdns_resolutions | how many domains seen on the IP in the last 24 hours |
| bad_pdns_resolutions | how many confirmed bad domains seen on the IP in the last 24 hours (used to create hotlist with filter) |
| total_domains | total number of domains see on this IP in the last 30 days |
| third_party_threats | number of domains on IP that are confirmed with any threat on 3rd party intel feed |
| allthreats_combined_percent | percentage of domains that are confirmed or predicted malicious |
| combined__phishing_percent | percentage of domains confirmed or predicted as phishing |
| combined_malware_percent | percentage of domains confirmed or predicted as malware |
| combined_spam_percent | percentage of domains confirmed or predicted as spam |
| asn | the IP's ASN (i.e. routing provider) |
| organization | organization associated with IP range based on Geo Data Partner |
| city | city based on IP Geo Data Partner |

| | |
|---|---|
| region | region based on IP Geo Data Partner |
| country | country based on IP Geo Data Partner |
| latitude | Coordinates |
| longitude | Coordinates |
| allthreats_combined_count | number of confirmed or predicted domains on 3rd party intel feed or threat profile |
| malicious_phishing | number of malicious phishing domains on 3rd party intel feeds |
| malicious_malware | number of malicious malware domains on 3rd party intel feeds |
| malicious_spam | number of malicious spam domains on 3rd party intel feeds |
| compromised_phishing | number of compromised phishing domains on 3rd party intel feeds |
| compromised_malware | number of compromised malware domains on 3rd party intel feeds |
| compromised_spam | number of compromised spam domains on 3rd party intel feeds |
| predicted_phishing | number of domains (with no confirmed threat) that we predict as phishing |
| predicted_malware | number of domains (with no confirmed threat) that we predict as malware |
| predicted_spam | number of domains (with no confirmed threat) that we predict as spam |
| allthreats_percent | Percentage of domains including all threat types |
| percent_phishing | percentage of domains that are confirmed phishing |
| percent_malware | percentage of domains that are confirmed malware |
| percent_spam | percentage of domains that are confirmed spam |
| zerolist_domains | number of zero listed domains seen on this IP |
| zerolist_ip | indicates if this IP is zero listed (e.g. CDN) |

**File Notes**

- One IP will be listed per line with the respective metadata fields
- The format of the file will be as follows:
  - IP <tab> meta_field1 <tab> meta_field2 <tab> meta_field3 <newline>
  - <newline> is a Unix-based newline character (“LF”, a.k.a. “\n”)

# Hosting IP Risk Feed File Acquisition

Hosting IP Risk Feed is available for daily download, directly from a transfer box managed by DomainTools, as a gzip-compressed, tab-separated CSV.

To gain access to the Hosting IP Risk Feed file, you will need to provide DomainTools with the following information:

- A customer email address
- One or more customer-owned static IP addresses from which all pull requests will be made.
- An SSH public key is generated and owned by the requesting customer. An RSA key of 2048 bits or higher is preferred.

The connections to the transfer box are made via SFTP using SSH and your key. DomainTools will add a configuration to allow access to our transfer boxes using a provided username and SSH key from the given. IP addresses.

The Hosting IP Risk Feed file is processed around 1:30 p.m. PDT each day, and requests should be made between 2:30 and 43:00 p.m. PDT, once daily.