User Guide

DomainTools IP Hotlist

DOMAINTOOLS®

IP Hotlist

DomainTools' prioritized list of active, high-risk IPs delivers predictive and deterministic insights that organizations can use to identify threats and defend their networks proactively.

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.

IP Hotlist Description

IP Hotlist is a list of IPs, appearing in ranked order, with the most concerning at the top. For each IP, the IP Hotlist 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.

IP Hotlist 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 feeds which provide known malicious domains as they are convicted on a daily basis.

IP Hotlist Contents

In summary, IP Hotlist will conform to the following requirements:

- The IP Hotlist will publish once daily
- Hotlist will contain IPs:
    - Associated with pDNS activity 1 day ago and resolved to known or predicted malicious domains
    - With percentages of known or predicted malicious domains is higher than 50% (Predicted Malicious Domains have a Risk score of 90 or higher; known malicious domains are domains that appear on a third-party threat intel feed as confirmed malicious)
- Hotlist will not contain IPs:
    - Associated with zero listed domains
    - From known CDN infrastructure
    - Or that host more than 10,000 domains to avoid including large hosting providers
- 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 45,000 and 60,000.
    - Domains hosted in the IP will be rescored each day and placed on the list according to the list's filtering parameters and rankings

IP Hotlist will be available in a tab-separated CSV file, containing the following information 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)

IP Hotlist File Acquisition

IP Hotlist 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 IP Hotlist 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 IP Hotlist 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.