User Guide

Domain Risk Score

Version 24.10

DomainTools

In this Document

This document explains the Domain Risk Score's components and how to interpret them.

Introduction

Domain Risk Score is powered by our real-time, historical database of observed changes in domain names, registrations, and infrastructure values. Our industry-leading data makes it possible for us to generate best-in-class analysis. We estimate a domain's observed connections to known-bad actors with Proximity, and its predicted risk with our Threat Profile suite of machine learning classifiers.

Our Proximity score measures a domain's observed closeness to known malicious domain infrastructure. We enrich known-bad domains with our own data, and reveal the innocent-looking domains to which they are linked. The Proximity score updates rapidly in response to changes in global DNS infrastructure.

Our Threat Profile uses machine learning (ML) classifiers to estimate the probability that a domain was registered with malicious intent, for the purpose of malware, phishing, and/or spam. We continuously refine our ML classifiers against changes in the global DNS and the

malicious domain landscape, drilling down to the signals (out of hundreds) most important for predicting malcine.

Domain Risk Score is fully incorporated into multiple DomainTools products for security automation and investigation.

Domain Risk Score Components

The Domain Risk Score components each score domains from 1-99. Proximity is a single 1-99 measure, and Threat Profile consists of one 1-99 score each for Phish, Malware, and Spam classifiers.

In the following example, the overall Domain Risk Score is taken from the highest of Proximity and Theat Profile. The Domain Risk Score inherits 81 from Threat Profile, which inherited 81 from Malware:

Domain Risk Score: 81
- Proximity: 23
- Threat Profile: 81
  - Malware: 81
  - Phish: 69
  - Spam: 1

No component of the Domain Risk Score definitively confirms malicious activity–because threat actors may register many domains but only utilize a few for malicious purposes. Nevertheless, the Domain Risk Score can help you identify the domains registered by threat actors, regardless of whether they are ultimately used for malicious activities.

Further context on interpreting Domain Risk Scores and their components is below.

Proximity

The Proximity score quantifies the closeness of a domain to known-malicious domains. It provides an indication of the likelihood that a domain is associated with malicious intent, based on signals from the domain's registration details and hosting infrastructure.

Proximity assigns risk much like a human investigator: looking at the connections domains have to each other. For example, if a large percentage of domains on a given IP address are malicious, the other domains on that IP address are assumed to be malicious.

Threat Profile

The Threat Profile is a set of machine learning (ML) classifiers that predict if a domain was registered with malicious intent. Consult our Domain Risk Score Technical Brief for more information about the design and testing of our machine learning tools.

The Threat Profile contains three components, each scored 1-99. Each classifier assesses the similarity between a domain's inherent characteristics and those associated with the following activities. The Threat Profile Score only applies to domains of an age of 28 months or younger.

Phish

A machine learning algorithm tuned to look for phishing-related domains: domains which may try to deceive a user by pretending to represent a product or service in order to perform malicious activities against a user.

Malware

A machine learning algorithm tuned to look for malware-related domains: domains used as part of malware hosting, dropping, command-and-control, or other activities.

Spam

A machine learning algorithm tuned to look for spam-related domains: domains part of spam email creation, distribution, or tracking.

Provisional Domain Risk Score

When a new domain is identified, DomainTools assigns a Provisional Domain Risk Score while the Threat Profile machine learning (ML) model processes the domain. Generally, domains that are less than 24 hours old will (temporarily) show this provisional score.

Domain Risk Score Ranges

Domain Risk Scores are a crucial part of your broader security toolset. DomainTools does not assess or condone the quality of the *content* hosted on scored domains.

Score Range	Score Color	Description
100	Red	Blocklisted. These domains can be considered known-bad, and have the highest likelihood of malicious intent. DomainTools combines third party blocklists with our own scoring to determine which domains to blocklist.
90-99	Red	Strong confidence in near-term weaponization.
70-89	Orange	A potential threshold for suggesting malicious intent, and our default recommendation for significance in an investigation. Individual mileage may vary, depending on your security context and priorities.
50-69	Yellow	May require attention, depending on your security posture.
1-49	Grey	Very little evidence of malicious intent.
0	Grey	Zero-listed. DomainTools zero-lists a domain when we have no evidence that it was registered with malicious intent. Zero-listing guards well-known legitimate domains against accidental blocking and includes domains which are vital to the expected operation of the Internet.

Using the Risk Score

The Domain Risk Score is fully integrated into our suite of Iris Products: Investigate, Enrich, and Detect.

Iris Intelligence Platform: UI and API

The Domain Risk Score is fully integrated into the DomainTools family of Iris products: Investigate, Enrich, and Detect. Risk scores appear for all active domains both in the web application user experience as well as in all Iris APIs.

Risk Score API Endpoints

The Domain Risk Score also has its own API endpoints, and is included in Iris API products. Consult our API documentation for more information.

Threat Intelligence Feeds

Domains with high risk scores can be downloaded for offline processing via our Threat Intelligence Feeds.

Integrations

Domain Risk Score is built into our third-party integrations, such as Splunk. Consult our Integrations page for more information.