DOMAINTOOLS

Domain Risk Score

Proactively uncover threats using DNS and data science

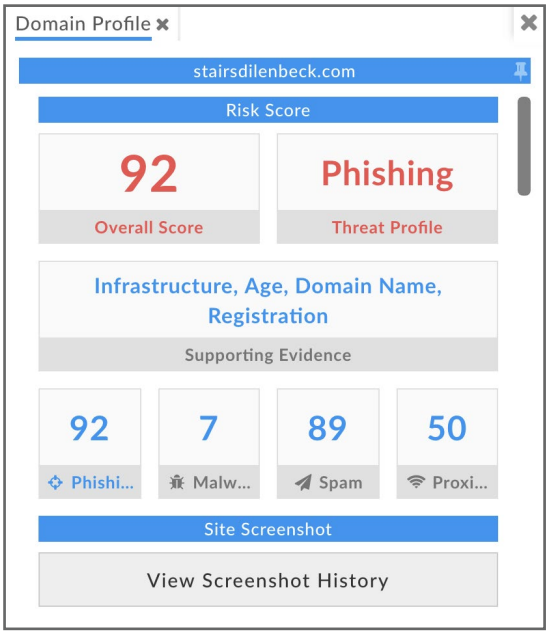
Predicting Malicious Domains

- What if you could reduce the false positives creating alert fatigue?
- What if you could tell at the moment of registration that a domain was going to cause harm?
- What if you knew that a domain name was hosted in a 'bad neighborhood' and was likely to be used for nefarious purposes?

Introducing Domain Risk Score

Today's threat environment demands a fast, reliable, automated way to assess and report the risk levels of domains so that appropriate security measures can be enacted ahead of attacks. DomainTools has developed proprietary technology, using a combination of data science and our market-leading DNS datastores, to do just this.

Most risk feeds are reactive rather than predictive. They require someone to be hurt before the domain lands on a reputation list. The Domain Risk Score, on the other hand, predicts the risk level and likely threats from a domain that has not been observed in malicious activities, by analyzing various properties of the domain that exist as soon as the domain is registered. The score comes from two distinct algorithms: Proximity examines how closely related a domain name is to other known-bad domains, while Threat Profile leverages machine learning to model how likely a domain name was created for malware, phishing, or spam purposes.



Domain Risk Score enhances understanding of domains in Iris

 | sales@domaintools.com | (206) 838-9020 | www.domaintools.com

Proximity

Our Proximity algorithm analyzes registration and hosting details for their connection to known-evil domains, and any other domain sharing those properties receives an elevated risk score. Malicious or dangerous domains are usually controlled by organizations with many domains in their holdings—"lone wolves" are uncommon. Therefore, if "Domain A" is observed to be malicious, then other domains controlled by the same organization ("Domain B," Domain C," etc) automatically inherit an elevated risk profile.

Threat Profile

Threat Profile is a set of state-of-the-art machine learning algorithms which model or "profile" the online holdings of bad actors, including domain registration and malicious infrastructure design. Our algorithms examine intrinsic properties of a domain as indicators of whether it fits one of our threat profiles: spam, malware, or phishing. We then predict whether a domain was registered with malicious intent—to be used as part of a campaign by a bad actor. Not all such domains are weaponized—many remain dormant. But because our algorithms analyze properties that are present from the moment the domain comes into existence, the technology can score domains without relying on published reports of malicious activity.

A Service You Can Count On

DomainTools is delivering next-generation predictive risk technology in our Domain Risk Score. The Risk Score is built upon the world's largest repository of current and historical domain information and advanced machine learning technologies to help organizations advance their prevention efforts proactively.

The Domain Risk Score has been designed and built to be accurate, reliable, efficient, and scalable. DomainTools risk scoring is used in production today by top-tier security organizations worldwide.

Want to Learn More?

To test the power of the DomainTools Risk Score or to get pricing information, email sales@domaintools.com or call 206-838-9020.