DNSDB from DomainTools

Cybercriminals know all about your infrastructure. How much do you know about theirs?

DNSDB is the world's largest passive DNS database, providing a unique, multifaceted view of global Internet infrastructure. With access to this critical intelligence, security teams gain unmatched insight into how threats emerge and evolve over time.

- **2TB** DNS data collected daily
- **100+ billion** DNS records
- **800k+** observations per second
- **1Gb/sec** real-time streaming data

ELIMINATE BLIND SPOTS

View Internet infrastructure to see how adversaries have rolled through domains, IP addresses, and name servers to conceal their activity

STOP PHISHING, MALWARE, AND RANSOMWARE EARLIER

Proactively defend your organization from sophisticated cyber threats.

MINIMIZE RISK

Access real-time and historical passive DNS data to block your infrastructure from being used by bad actors.

Access methods to suit your workflow

DNSDB API

Unlock the power of DNS intelligence across dozens of SIEM, SOAR, and threat intelligence platforms.

Features and Benefits:

- Ability to search RRname, RRdata, and by IPv4 or IPv6 address or address block
- Support for whole-label left-hand-side or right-hand-side domain name wildcards
- Support for IP range or CIDR prefix RRdata searches
- Able to return up to a million results per query
- Flexible Search and support for regular expressions

DNSDB EXPORT

Download an on-premise installation of DNSDB in your own environment or a hosted service.

Features and Benefits:

- Full DNSDB Flexible Search and Standard Search functionality
- Total query privacy for compliance with industry regulations
- Ability to access data in an offline environment
- Unlimited query volume
- Minimal network latency
- Fastest response time

DomainTools

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.