August 2021

Domain Discovery Feed User Guide

DOMAINTOOLS®

Domain Discovery Feed

DomainTools now offers a simple way to consume newly registered domains using the industry's most comprehensive domain discovery platform to help organizations mitigate threats posed by young domains.

Comprehensive New Domain Detection

The DomainTools Domain Discovery Feed goes beyond known zone files, leveraging over 20 years of experience gathering, processing, and provisioning domain-related data. DomainTools' unique capabilities include multiple methods to detect the presence of new domains, providing the most complete feed for new domain registrations. Registered domains are made available via the processing of Zone Files and other official data sources. In contrast, discovered domains include those identified via proprietary mechanisms which are not in the scope of competing solutions.

Description

The Domain Discovery Feed is a flat file containing a list of domains that were registered or discovered in the previous 24 hours.

Use Cases

Because it is a simple list of domain names, the Domain Discovery Feed is highly versatile and may be suitable for a variety of applications, including:

- **Blocking Rules:** Maximum flexibility for using the new domain information to create alerting or blocking rules for network or host defenses.
- **Alerting:** Security Information Event Management (SIEM) platforms, Threat Intelligence Platforms (TIP), and a variety of other log and event aggregation sources can capture domains accessed from the protected environment; scripts that check these domains against the Domain Discovery Feed can then raise alerts when traffic to matching domains is observed.
- **Zero Trust:** In some environments, a zero-trust policy toward new domains is employed; in such cases, the Domain Discovery Feed can enable the creation of automatic blocking rules for most traffic or quarantine/inspection rules for SMTP and other protocols that can accommodate various dispositions.

Domain Discovery Feed File Acquisition

The feed is available for daily download, directly from a transfer server managed by DomainTools, as a gzip-compressed, text file in CSV format.

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

- A customer email address.
- One or more customer-owned static IP addresses (preferably a /32 address) from which all pull requests will be made.
- An SSH public key that is generated and owned by the requesting customer. An RSA key of at least 4096 bits is preferred.

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

Example connection request to retrieve the file:

```
sftp -i <YOUR_IDENTITY_FILE> <YOURUSERNAME>/@transfer.domaintools.com
```

The file is processed at 8:00 AM Pacific Time each day, requests made after this time should return the newest file. Processing time may vary depending on the data volumes but generally does extend past 12:00 PM Pacific Time.