# WhoisXML API Now Offers 6 Files for its DNS Database Download Service

Posted on July 2, 2021

WhoisXML API made its DNS database download available in six different files, each for different DNS record types. Doing so makes the DNS database files easier to integrate and analyze and enables particular use cases.

The resource records you can download as database files are:

- **A records:** An A record directs a domain or subdomain to an IP address. It is possibly the most basic type of DNS record, as all domains should resolve to an IP address to become accessible.
- **Mail exchanger (MX) records:** This type of record specifies the mail server where email messages meant for a specific domain are accepted.
- **Nameserver (NS) records:** The NS record determines the authoritative DNS server for the domain name.
- **Text (TXT) records:** This type of DNS record was initially allotted for human-readable information about a domain that serves as notes for administrators. Its use has, however, evolved to include serial numbers, codes, and server names.
- **Canonical name (CNAME) records:** A CNAME allows website administrators to provide aliases to domain names by pointing them to another domain. The domain blog[.]example[.]com, for example, can be given the alias or CNAME example[.]com.
- **Start of Authority (SOA) records:** SOA records contain administrative details about a particular domain's zone. This record helps manage zone transfers and contains the primary nameserver, serial numbers, and timestamps.

This tutorial looks into the six types of DNS databases now available for download.

## How to Access DNS Database Download

Accessing WhoisXML API's DNS databases requires a subscription. To get started, contact us or send an email to sales@whoisxmlapi.com. If you already have an account, follow the steps below.

- Go to https://reverse-ip.whoisxmlapi.com/database.
- Click the "Order database" button.




- On the list of subscribed data feeds that appears, select DNS Database Download.



**Directory of https://reverse-ip.whoisxmlapi.com/datafeeds/**

```
Login successful.

          4 Nov 08  2019 All_Registered_Domains
      12288 Jun 14 16:59 DNS_Database_Download
        152 Oct 15  2019 Daily_Website_Contacts_and_Categorization
      36864 Jun 15 12:01 Disposable_Email_Domains
     331776 Jun 16 06:16 IP_Netblocks_WHOIS_Database
          9 Feb 24 17:03 Newly_Registered_Domains
       8192 Jun 16 05:00 Subdomains_Database
     233472 Jun 16 03:34 Typosquatting_DataFeed
```

- Select the type of DNS database you want to download. Clicking on a specific file name automatically starts the download.

## Understanding the File Naming Conventions

The databases follow this file naming format: dns_[record type]_database.[date].[file type].csv.gz where:

- **Record type:** Refers to the resource record found in the database, such as A, SOA, TXT, NS, MX, or CNAME. For the DNS A Database, this field is left blank, so the name becomes dns_database.
- **Date:** The date when the file was generated.
- **File type:** This field could be “full,” which means you will be downloading the entire database, regardless of date. It could also be “weekly.diff” or “monthly.diff,” which means it only contains the new records found within the week or month specified.

| | | | | |
|---|---|---|---|---|
| 2625498019 | Jun | 14 | 07:22 | dns_mx_database.2021-06-14.full.csv.gz |
| 59897726 | Jun | 14 | 14:00 | dns_mx_database.2021-06-14.weekly.diff.csv.gz |
| 8950307007 | May | 17 | 12:30 | dns_ns_database.2021-05-17.full.csv.gz |
| 161702626 | May | 18 | 07:09 | dns_ns_database.2021-05-17.weekly.diff.csv.gz |
| 8980382265 | May | 24 | 06:54 | dns_ns_database.2021-05-24.full.csv.gz |
| 128101182 | May | 24 | 15:46 | dns_ns_database.2021-05-24.weekly.diff.csv.gz |
| 8951269464 | May | 31 | 07:24 | dns_ns_database.2021-05-31.full.csv.gz |
| 109765467 | May | 31 | 16:23 | dns_ns_database.2021-05-31.weekly.diff.csv.gz |
| 8870237245 | Jun | 07 | 07:09 | dns_ns_database.2021-06-07.full.csv.gz |
| 411809490 | Jun | 07 | 19:05 | dns_ns_database.2021-06-07.monthly.diff.csv.gz |
| 30341533 | Jun | 07 | 18:04 | dns_ns_database.2021-06-07.weekly.diff.csv.gz |
| 8847911991 | Jun | 14 | 08:31 | dns_ns_database.2021-06-14.full.csv.gz |
| 161458750 | Jun | 14 | 14:31 | dns_ns_database.2021-06-14.weekly.diff.csv.gz |
| 4036592957 | May | 18 | 13:48 | dns_soa_database.2021-05-17.full.csv.gz |
| 4416727316 | May | 24 | 05:27 | dns_soa_database.2021-05-24.full.csv.gz |
| 814669103 | May | 24 | 15:21 | dns_soa_database.2021-05-24.weekly.diff.csv.gz |
| 4709084643 | May | 31 | 06:26 | dns_soa_database.2021-05-31.full.csv.gz |
| 868944728 | May | 31 | 15:55 | dns_soa_database.2021-05-31.weekly.diff.csv.gz |
| 4709084643 | Jun | 07 | 06:14 | dns_soa_database.2021-06-07.full.csv.gz |
| 4709084643 | Jun | 07 | 18:55 | dns_soa_database.2021-06-07.monthly.diff.csv.gz |
| 38 | Jun | 07 | 17:39 | dns_soa_database.2021-06-07.weekly.diff.csv.gz |
| 5023025555 | Jun | 14 | 06:53 | dns_soa_database.2021-06-14.full.csv.gz |
| 1036072321 | Jun | 14 | 14:12 | dns_soa_database.2021-06-14.weekly.diff.csv.gz |
| 3349652283 | May | 18 | 23:50 | dns_txt_database.2021-05-17.full.csv.gz |
| 4118093537 | May | 24 | 05:54 | dns_txt_database.2021-05-24.full.csv.gz |
| 3053675718 | May | 24 | 15:30 | dns_txt_database.2021-05-24.weekly.diff.csv.gz |
| 4707656441 | May | 31 | 06:26 | dns_txt_database.2021-05-31.full.csv.gz |
| 3101593871 | May | 31 | 16:05 | dns_txt_database.2021-05-31.weekly.diff.csv.gz |
| 4707656441 | Jun | 07 | 06:14 | dns_txt_database.2021-06-07.full.csv.gz |
| 4707656441 | Jun | 07 | 18:53 | dns_txt_database.2021-06-07.monthly.diff.csv.gz |
| 38 | Jun | 07 | 17:40 | dns_txt_database.2021-06-07.weekly.diff.csv.gz |
| 5254562769 | Jun | 14 | 06:52 | dns_txt_database.2021-06-14.full.csv.gz |
| 3265770199 | Jun | 14 | 14:24 | dns_txt_database.2021-06-14.weekly.diff.csv.gz |

## DNS Databases Available from WhoisXML API

The six types of DNS databases we offer are discussed in detail below. More information can also be found here.

## DNS A Database

Our DNS A Database contains the IP resolutions of domain names. These files are labeled “dns_database” on the main download page. The database has three columns, namely:

- **d:** Lists all domain names.
- **du:** The date and timestamp when the DNS record was last updated.
- **ips:** The IP addresses the domains resolve to. If a domain resolved to multiple IP addresses in the past, all these IP addresses are reflected in this column.

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| 1 | DOMAIN | LAST_UPDATE_TIMESTAMP | IPS | | | | | | |
| 733 | broadband-5-228-162-108.ip.moscow.rt.ru | 1564119709 | 5.228.162.108 | | | | | | |
| 734 | b-group.site | 1564118413 | 31.31.196.118 | | | | | | |
| 735 | biggboss11auditions2017.xyz | 1564118836 | 219.94.224.112 | 49.212.124.161 | | | | | |
| 736 | bestof-tgp.com | 1564118705 | 195.56.193.78 | | | | | | |
| 737 | bedroomblinds.co.uk | 1564118628 | 52.16.25.241 | | | | | | |
| 738 | blueponds.com | 1564119086 | 45.56.111.241 | | | | | | |
| 739 | bestoflbi.buzz | 1564118663 | 216.15.222.111 | | | | | | |
| 740 | biggirlproduction.net | 1564118748 | 104.17.202.73 | 104.17.203.73 | 104.17.204.73 | 104.17.205.73 | 104.17.206.73 | | |
| 741 | b-internet.176.48.180.10.nsk.rt.ru | 1564117719 | 87.239.45.231 | | | | | | |
| 742 | bko1908.com | 1564118845 | 23.236.62.147 | | | | | | |
| 743 | broadband-188-32-112-12.ip.moscow.rt.ru | 1564119689 | 188.32.112.12 | | | | | | |
| 744 | broadband-5-228-213-187.nationalcablenet | 1564119641 | 193.227.240.131 | | | | | | |
| 745 | bonedrone.buzz | 1564119193 | 184.168.221.55 | | | | | | |

## DNS MX Database

DNS MX Database lists domain names and their corresponding mail servers. The file names for this database type begins with “dns_mx_database,” and has four columns:

- **d:** This column contains the domain names found for the selected date.
- **du:** The date and timestamp when the MX record was last updated is reflected here.
- **pr:** This refers to the priority or preference in which the specific mail server should be used, 1 being the highest priority and 100, the lowest. Setting mail server priority enables load sharing between primary and backup mail servers.
- **mx:** This column lists the mail server associated with the domain name.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | d | du | pr | mx | | |
| 9091 | 007kitchens.com | 1608996526 | 10 | mx00.1and1.com | | |
| 9092 | 007kitchens.com | 1608996526 | 10 | mx01.1and1.com | | |
| 9093 | 007kleening.com | 1608996218 | 10 | mx00.ionos.co.uk | | |
| 9094 | 007kleening.com | 1608996218 | 10 | mx01.ionos.co.uk | | |
| 9095 | 007kn.com | 1607645896 | 10 | mx156.hostedmxserver.com | | |
| 9096 | 007kush.com | 1608996469 | 0 | localhost | | |
| 9097 | 007lab.com | 1608996183 | 1 | localhost | | |
| 9098 | 007lab.com | 1608996183 | 1 | mx247.in-mx.com | | |
| 9099 | 007lab.com | 1608996183 | 1 | mx247.in-mx.net | | |
| 9100 | 007labs.co.uk | 1608996272 | 10 | mxs1.xsmtpserver.net | | |
| 9101 | 007labs.co.uk | 1608996272 | 20 | mxs2.xsmtpserver.net | | |
| 9102 | 007lan.com | 1604016875 | 10 | mx156.hostedmxserver.com | | |
| 9103 | 007laohujixiaoyouxi.cryy120 | 1608996190 | 1 | mail.happyisp.com | | |
| 9104 | 007laohujixiaoyouxi.zhycn.c | 1608996170 | 1 | mail.happyisp.com | | |
| 9105 | 007law.co.nz | 1608996177 | 10 | mx.partnerconsole.net | | |
| 9106 | 007law.co.nz | 1608996177 | 20 | mx4.partnerconsole.net | | |
| 9107 | 007leinuo.com | 1608996400 | 10 | mx156.hostedmxserver.com | | |
| 9108 | 007let.com | 1608996423 | 5 | mail.007let.com | | |
| 9109 | 007liaomendeduchang.pock | 1607645642 | 1 | mail.happyisp.com | | |
| 9110 | 007liaomendeduchang.zhan | 1608996819 | 1 | mail.happyisp.com | | |
| 9111 | 007licenseplate.com | 1608996274 | 0 | mail.007licenseplate.com | | |

### DNS NS Database

This type of DNS database download helps you map out the NSs associated with a particular domain name. The file names begin with “dns_ns_database,” and contain three columns:

- **d:** Lists all domain names.
- **du:** Contains the date and timestamp of the last update made.

- **ns:** This column includes the NSs associated with the domains listed in the first column.

| | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | d | du | ns | | |
| 658 | 0-163-129-45.customers.atlantis.it | 1608996372 | ns1.sedoparking.com | | |
| 659 | 0-163-129-45.customers.atlantis.it | 1608996372 | ns2.sedoparking.com | | |
| 660 | 0-169.com | 1607646022 | ns1.register.it | | |
| 661 | 0-169.com | 1607646022 | ns2.register.it | | |
| 662 | 0-169.com | 1607646022 | suspended1.plaindns.net | | |
| 663 | 0-169.com | 1607646022 | suspended2.plaindns.net | | |
| 664 | 0-18.dk | 1608996211 | ns01.servage.net | | |
| 665 | 0-18.dk | 1608996211 | ns02.servage.net | | |
| 666 | 0-18.dk | 1608996211 | ns03.servage.net | | |
| 667 | 0-18.dk | 1608996211 | ns04.servage.net | | |
| 668 | 0-18.dk | 1608996211 | ns05.servage.net | | |
| 669 | 0-185.biz | 1608996286 | ns10.wixdns.net | | |
| 670 | 0-185.biz | 1608996286 | ns11.wixdns.net | | |
| 671 | 0-186-138.nrttelecom.com.br | 1608996430 | ns1.nrttelecom.com.br | | |
| 672 | 0-186-138.nrttelecom.com.br | 1608996430 | ns2.nrttelecom.com.br | | |
| 673 | 0-18egitimdanismanlik.online | 1608996664 | ns1.natrohost.com | | |
| 674 | 0-18egitimdanismanlik.online | 1608996664 | ns2.natrohost.com | | |
| 675 | 0-18klinik.com | 1608996398 | ns1.natrohost.com | | |
| 676 | 0-18klinik.com | 1608996398 | ns2.natrohost.com | | |

### DNS TXT Database

TXT records contain text information about the domain and may serve several purposes, including domain ownership verification and spam prevention. Our DNS TXT Database (signified by the string “dns_txt_database” in their names) has three columns, namely:

- **d:** This column lists the domain names.

- **du:** This refers to the date and timestamp when the TXT record was last updated.
- **txt:** Contains the TXT record detail specified by the domain administrator. If a domain has multiple TXT records, each one is displayed in a different row.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | d | du | txt | | | | | | | | | | | |
| 8603 | 0-24automento.hu | 1619829675 | \|v=spf1 ip4:185.111.89.226 include:mail.cpanel31.tarhelypark.hu +a +mx +ip4:185.51.67.19 +ip4:185.51.67.22 ~alla.online | | | | | | | | | | | |
| 8604 | 0-24automento.hu | 1619829675 | \|v=spf1 ip4:185.111.89.226 include:mail.cpanel31.tarhelypark.hu +a +mx +ip4:185.51.67.19 +ip4:185.51.67.22 ~allne | | | | | | | | | | | |
| 8605 | 0-24automento.hu | 1619829675 | \|v=spf1 ip4:185.111.89.226 include:mail.cpanel31.tarhelypark.hu +a +mx +ip4:185.51.67.19 +ip4:185.51.67.22 ~allnline | | | | | | | | | | | |
| 8606 | 0-24automento.hu | 1619829675 | \|v=spf1 ip4:185.111.89.226 include:mail.cpanel31.tarhelypark.hu +a +mx +ip4:185.51.67.19 +ip4:185.51.67.22 ~allom | | | | | | | | | | | |
| 8607 | 0-24automento.hu | 1619829675 | \|v=spf1 ip4:185.111.89.226 include:mail.cpanel31.tarhelypark.hu +a +mx +ip4:185.51.67.19 +ip4:185.51.67.22 ~allz pw | | | | | | | | | | | |
| 8608 | 0-24domain.hu | 1619830085 | \|mail.0-24domain.hu | | | | | | | | | | | |
| 8609 | 0-24domain.hu | 1619830085 | \|mail.0-24domain.hu.com | | | | | | | | | | | |
| 8610 | 0-24domain.hu | 1619830085 | \|mail.0-24domain.hucom | | | | | | | | | | | |
| 8611 | 0-24domain.hu | 1619830085 | \|mail.0-24domain.huite | | | | | | | | | | | |
| 8612 | 0-24gazkeszulek.hu | 1619742202 | \|v=spf1 a mx ip4:185.6.139.29 a:s029.mailpool.netmask.hu ~all | | | | | | | | | | | |
| 8613 | 0-24gazkeszulek.hu | 1619742202 | \|v=spf1 a mx ip4:185.6.139.29 a:s029.mailpool.netmask.hu ~allnaws.com | | | | | | | | | | | |
| 8614 | 0-24huto.hu | 1619741905 | \|v=spf1 a mx ip4:185.6.139.29a:{$servename}.mailpool.{$domain} ~all | | | | | | | | | | | |
| 8615 | 0-24mosogatogep.hu | 1619741791 | \|v=spf1 a mx ip4:185.6.139.29 a:s029.mailpool.netmask.hu ~allV | | | | | | | | | | | |

## DNS CNAME Database

Website administrators can make multiple domains and subdomains point to the same application or page within the same server by setting up CNAME records. Our DNS CNAME Database keeps track of such records to help you see which domains have CNAME records and what domains they point to.

This type of database has the string “dns_cname_database” in their names and has three columns:

- **d:** This column lists all domain names.
- **du:** Contains the date and timestamp when the CNAME record was last updated.
- **cname:** Lists the domain that the corresponding domain identified in the first column points to.

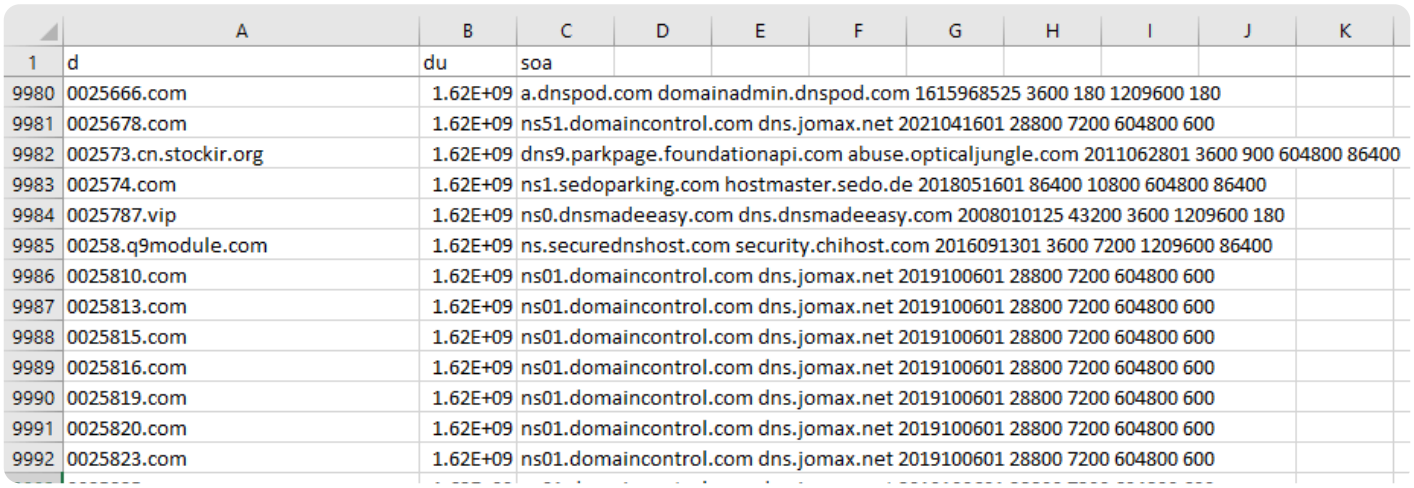
| | A | B | C | D |
|---|---|---|---|---|
| 1 | d | du | cname | |
| 160 | 0-171-118-80.escort.fr | 1619741872 | escort.fr | |
| 161 | 0-171.rkcom.net | 1619742051 | comtrance.net | |
| 162 | 0-172.rkcom.net | 1619741946 | comtrance.net | |
| 163 | 0-173-227-188.rackcentre.redsta | 1619741874 | redstation.com | |
| 164 | 0-174.rkcom.net | 1619742711 | comtrance.net | |
| 165 | 0-176-227-188.rackcentre.redsta | 1619742092 | redstation.com | |
| 166 | 0-177-243-80.rackcentre.redstati | 1619741733 | redstation.com | |
| 167 | 0-177.rkcom.net | 1619741774 | comtrance.net | |
| 168 | 0-178-243-80.rackcentre.redstati | 1619741943 | redstation.com | |
| 169 | 0-178.rkcom.net | 1619741789 | comtrance.net | |
| 170 | 0-179-227-188.rackcentre.redsta | 1619742033 | redstation.com | |
| 171 | 0-18-200-109.rackcentre.redstati | 1619742371 | redstation.com | |
| 172 | 0-18.com.pagesstudy.com | 1619741859 | pagesstudy.com | |
| 173 | 0-18.gr.pagesstudy.com | 1619741817 | pagesstudy.com | |
| 174 | 0-18.ru.pagesstudy.com | 1619742032 | pagesstudy.com | |
| 175 | 0-180-227-188.rackcentre.redsta | 1619741722 | redstation.com | |

### DNS SOA Database

This type of database contains the SOA records of domain names that contain administrative details about the zone. File names start with “dns_soa_database,” and files have three columns:

- **d:** Refers to the domain names in the database.
- **du:** This column contains the date and timestamp when the SOA record was last updated.

- **soa:** Lists the SOA record associated with the domain indicated in the first column.



| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | d | du | soa | | | | | | | | |
| 9980 | 0025666.com | 1.62E+09 | a.dnspod.com domainadmin.dnspod.com 1615968525 3600 180 1209600 180 | | | | | | | | |
| 9981 | 0025678.com | 1.62E+09 | ns51.domaincontrol.com dns.jomax.net 2021041601 28800 7200 604800 600 | | | | | | | | |
| 9982 | 002573.cn.stockir.org | 1.62E+09 | dns9.parkpage.foundationapi.com abuse.opticaljungle.com 2011062801 3600 900 604800 86400 | | | | | | | | |
| 9983 | 002574.com | 1.62E+09 | ns1.sedoparking.com hostmaster.sedo.de 2018051601 86400 10800 604800 86400 | | | | | | | | |
| 9984 | 0025787.vip | 1.62E+09 | ns0.dnsmadeeasy.com dns.dnsmadeeasy.com 2008010125 43200 3600 1209600 180 | | | | | | | | |
| 9985 | 00258.q9module.com | 1.62E+09 | ns.securednshost.com security.chihost.com 2016091301 3600 7200 1209600 86400 | | | | | | | | |
| 9986 | 0025810.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |
| 9987 | 0025813.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |
| 9988 | 0025815.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |
| 9989 | 0025816.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |
| 9990 | 0025819.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |
| 9991 | 0025820.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |
| 9992 | 0025823.com | 1.62E+09 | ns01.domaincontrol.com dns.jomax.net 2019100601 28800 7200 604800 600 | | | | | | | | |

## DNS Databases in Action: What Attacks Can They Help Prevent?

### DNS Hijacking

DNS hijacking or redirection is a type of DNS attack where malicious actors change the victims' DNS settings to redirect them to malicious websites or applications. One example of malware that makes DNS hijacking possible is DNSChanger, which can replace a domain's NS with one that points to a malicious IP address.

DNS databases, specifically DNS NS and A Databases, can help you check which domains have possibly been redirected to malware-carrying IP addresses and NSs.

### Malware

Aside from DNS hijacking, threat actors very often use malware, including ransomware, to carry out attacks. Changing the DNS settings of a victim's computer may enable threat actors to plant

data-stealing and -locking malware on their systems.

With a DNS database, security teams can check for domains that resolve to IP addresses associated with ransomware and other malware. For example, in the sample DNS A Database, three domains point to 50[.]63[.]202[.]39, an IP address cited for its involvement in ransomware and other malicious campaigns. These domains are:

- alextandang[.]com
- celltechsvcs[.]com
- youngswagclothes[.]com

The timestamps on the database can provide more context on associations between domains and the malicious IP address.

### Spam Campaigns and Email Spoofing

TXT records can be used to enhance email security by making it a space for specifying Sender Policy Framework (SPF) records and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) authentication. Blank TXT records or unspecified SPF records can make a domain vulnerable to spoofing and cause emails to be marked as spam.

---

We will continue to make our DNS database download services available in easily accessible and consumable formats. Our goal is to help cybersecurity teams, investigators, and researchers identify threats, uncover artifacts, and map out associations between malicious records.