DNS Database Download Is Now Reinforced with Wildcard and Active Fields

Posted on November 12, 2024

We are excited to announce that the Standard and Premium DNS Database files from DNS Database Download are now enriched with two new columns, namely, **wildcard** and **active**. These additions allow you to determine if a DNS record is part of a wildcard entry and check if a domain name or subdomain is active based on its most recent resolution status.

d	du	ips	wildcard	active
0-wv.codespot.com	1728757225	2607:f8b0:4023:c0b::52	TRUE	TRUE
0001098fef8c68ac1c5dc516.keenetic.io	1728827580	2a00:ab00:1103:20::50 2a03:21c0:0:227::96	TRUE	TRUE
0002cf78f3ec9afda6b30558.keenetic.io	1728831002	2a00:ab00:1103:20::50 2a03:21c0:0:227::96	TRUE	TRUE
00169e036d5d7f2a62bd57ac036643fe.fedramp.r2.cloudflarestora	1728857391	2606:4700:78::90:0:180 2606:4700:78::90:0:181 2606:4700	TRUE	TRUE
002.vicd.eu.org	1728578572	2606:4700:3030::ac43:a851 2606:4700:3033::6815:5e8a	TRUE	TRUE
00217226e037f494c269af5e.keenetic.io	1728720513	2a01:4f8:271:5a5c:: 2a01:4f9:3b:29a0::	TRUE	TRUE
002e283870250c35a99c2f4a06af5910.eu.r2.cloudflarestorage.co	1728859258	2a06:98c1:3200::90:0 2a06:98c1:3200::90:1 2a06:98c1:320	TRUE	TRUE
002e283870250c35a99c2f4a06af5910.r2.cloudflarestorage.com	1728859258	2606:4700:7::ec 2a06:98c1:58::ec	TRUE	TRUE
004c1e85a488d36e1ef2ecafa0810f3f.fedramp.r2.cloudflarestorag	1728852625	2606:4700:78::90:0:180 2606:4700:78::90:0:181 2606:4700	TRUE	TRUE
004c2a861e17991930081302.keenetic.io	1728837547	2a00:ab00:1103:20::50 2a03:21c0:0:227::96	TRUE	TRUE
005232f996c4d331304a91c4.keenetic.io	1728581027	2a00:ab00:603:45::19 2a00:ab00:1103:20::50	TRUE	TRUE
00555c4cdb32bbf51ce2764c.keenetic.io	1728714901	2a00:ab00:1103:20::50 2a03:21c0:0:227::96	TRUE	TRUE
0057f8ae6d69c7168c37b8ce.keenetic.io	1728773302	2a00:ab00:603:45::19 2a03:21c0:0:227::96	TRUE	TRUE
0-11235.com	1728663261	2400:b800:7::22	FALSE	TRUE
0-9.au	1728741527	2400:b800:3:1::43	FALSE	TRUE
00.com.ua	1728783916	2606:4700:3030::ac43:c658 2606:4700:3037::6815:5a5a	FALSE	TRUE

If the **wildcard** column says **True**, a query for a random FQDN has returned a DNS record. Therefore, the domain is expected to have a wildcard DNS configuration. On the other hand, a **False** value in the column means only defined subdomains resolve to specific DNS records. Queries for random FQDNs will not return corresponding DNS records. An empty **wildcard** column signifies the domain's DNS records have not yet been checked.

With this new **wildcard** field, WhoisXML API users can now:

- **Better filter out DNS data noise**: A wildcard subdomain, or catch-all subdomain, can generate DNS entries for many non-existent subdomains. As such, the new **wildcard** field enables you to focus only on subdomains created by DNS record administrators. This feature leads to a cleaner and better-quality dataset that requires lower storage and processing requirements.

- **Expand attack surface discovery**: Wildcard subdomains can pose security risks, especially if unknown to security teams, and can be abused by attackers. Therefore, identifying them through DNS intelligence can help reduce your attack surface by avoiding their use or, if strictly necessary, limiting and closely monitoring them.

Meanwhile, the new **active** field helps users determine if a DNS record exists for the domain of interest. If the field says **True**, queries to the DNS server have returned a valid DNS record and the domain is considered active. However, if the queries returned an error saying no DNS records were retrieved, the domain is inactive and the field will be marked **False**. An empty **active** column means that the domain's DNS records have not yet been checked.

The **active** field enables users to:

- **Enhance cyber investigations**: Analyzing the timestamps of a malicious domain's recent or historical resolutions, along with whether these resolutions were successful or failed, can help investigators reconstruct a timeline of events relevant to a cyber incident. The data can further be used as forensic evidence.

- **Identify botnets and DGA-created domains**: Various DNS requests that do not lead to resolutions may indicate that DGA-based botnet activity is ongoing. Therefore, monitoring the number of failed DNS resolutions can help with endpoint protection.

- **Detect malware distribution**: Malicious domains often have fluctuating resolution statuses as they are rapidly weaponized and frequently taken down soon after. Tracking these changes can help identify an attacker's tactics, techniques, and procedures (TTPs).

In summary, both **wildcard** and **active** data points can empower you to refine your DNS data analyses, identify potential security risks, and enhance your overall security posture. These new

fields are also available as optional output parameters for several of our APIs such as Reverse IP API, Reverse DNS API, Reverse MX API, and Reverse NS API.

Download a sample of our Premium DNS Database files or contact us for a better overview of the new "wildcard" and "active" fields.