Our Passive DNS APIs Are Now Enriched with Wildcard and Active Output Parameters

Posted on December 4, 2024

We are thrilled to announce that several of our APIs have been upgraded to include new data points, namely, **wildcard** and **active**. In particular, both fields are now optional output parameters for Reverse IP API, Reverse DNS API, Reverse MX API, and Reverse NS API. Our newly launched DNS Chronicle API, meanwhile, has a **wildcard** field as part of its default output format.

When the **wildcard** field says **True**, a query for a random FQDN has led to a DNS record, meaning the domain is configured with a wildcard DNS entry. Conversely, if the field says **False**, queries for random FQDNs did not return corresponding DNS records and only predefined subdomains resolve to valid DNS records. An empty **wildcard** field means the domain's DNS records have not yet been checked.

With this newly introduced wildcard field, WhoisXML API users are now able to:

- **Reduce DNS data noise:** Wildcard entries may generate extensive lists of associated domains sharing common A, NS, MX, or other DNS records. Using the new **wildcard** field to filter out these entries can significantly enhance domain data quality and improve analysis efficiency.

- **Improve attack surface reduction efforts:** Wildcard DNS entries can inadvertently expand an organization's attack surface, as they can serve as potential attack entry points. Providing security teams visibility over these wildcard entries can help them proactively address risks, either by restricting wildcard use or implementing thorough monitoring.

On the other hand, the new **active** field allows users to determine if a DNS record exists for a given domain. If the field says **True**, queries to the DNS server returned a valid DNS record,

meaning the domain is active. However, if the queries returned errors or no DNS records were retrieved, the domain is considered inactive and the field will say **False**. An empty field means that the DNS records for the domain have not yet been checked.

The new **active** field allows users to:

- **Gain crucial insights for threat analyses:** The APIs can now determine whether a malicious domain's historical resolutions were successful. This information can help investigators more effectively document the incident timeline and potentially visualize the attack sequence with greater clarity.

- **Detect potential malicious activities:** Since the APIs return the resolution status of historical DNS queries, they can help identify multiple failed DNS resolutions that may indicate malicious domain activities, such as in DGA-based botnet requests and malware distribution.

Reverse IP API, Reverse DNS API, Reverse MX API, Reverse NS API, and DNS Chronicle API tap into our market-leading Premium DNS Database, which also reflects the new fields.

Test our Passive DNS APIs now or contact us for a better overview of the new "wildcard" and "active" fields.