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.

With the new wildcard field, WhoisXML API users can now:

- **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 **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.