Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Broaden Data-Centric Threat Detection and Response with WHOIS, IP, and DNS Intelligence

As the cyber threat landscape expands at every cover of the web, organizations are bound to be left open, at least temporarily, to emerging or yet-unknown vulnerabilities. The challenge for detection and response (D&R) service providers is to stay on top of every client's multidimensional threat environment. An extensive and timely view of the global Domain Name System (DNS) can help D&R teams and providers see everything better, including WHOIS, IP, and domain data to deepen incident and vulnerability analysis, enrich threat intelligence, and enable real-time monitoring.

1. Global Incident and Vulnerability Data Enrichment

With businesses closing down or losing vast sums of money due to cyber attacks, enterprises are confronted with the reality of cyber threats every day. Understandably, they demand top-notch vulnerability scanning features and extensive threat contextualization. This expectation is cascaded to D&R teams and service providers. How can comprehensive access to the world's DNS help build an in-house Internet data collection engine to provide the utmost protection?

Notable Use Cases	Connected Data Points
Add more context to cyber incidents	• What registrant organizations, names, email addresses, and other clues are currently and historically behind a suspicious or malicious domain? • What nameservers and IP resolutions did the malicious domain use at the time of the incident? When were these resolutions first and last seen? • How are the malicious domains categorized? What types of content do they host?
Uncover additional artifacts related to threat incidents	• What other domains and subdomains share the same digital footprints (e.g., nameserver, registrant information, Secure Sockets Layer (SSL) certificates, and text strings) as the suspicious or malicious properties? • Do the suspicious or malicious domains belong to a typosquatting group with look-alike domains registered on the same day? What other digital characteristics do they have in common (e.g., text strings, nameservers, registrars, etc.)? • What IP addresses do the threat indicators resolve to? Are there suspicious domains and subdomains on these IP addresses, too?

Assess the organization's vulnerability against threats specific to domains	• Do any of the client's domains have outdated security protocols? • Are there exploitable misconfigurations in the organization's SSL certificates? Are there inconsistencies in the complete SSL chain? • Are there misconfigurations in the client's domain infrastructure? What are the domains' risk scores? • Are the organization's domains protected with the appropriate status codes?
Assess the client's vulnerability against DNS threats	• Are there unused and outdated subdomains hosted on the client's root domains? Are there signs of dangling DNS records that could lead to subdomain takeovers? • Is the client's DNS infrastructure configured correctly, including nameservers, mail servers, and subnetworks? How vulnerable is it to DNS-based attacks, such as DNS hijacking? • Are the DNS records overly descriptive and leave too many breadcrumbs for threat actors? • To which IP addresses do the organization's domains resolve? Do they belong to safe IP ranges?

2. Real-Time Asset and Threat Monitoring

Every minute counts for cybersecurity. With the frequency of zero-day attacks reaching record highs, monitoring assets and threats in real-time is crucial so organizations can immediately address exploitable assets and avoid threats. As early threat and vulnerability detection is tantamount to threat prevention and risk reduction, a real-time stream of DNS intelligence can give enterprises an edge, reducing the risk of detecting attacks too late.

Notable Use Cases	Connected Data Points
Monitor assets and the DNS round-the-clock	• What domain names were registered in the past hour using the organization's email address? What registrars are responsible for the domains? Did the domain administrator authorize them? • Does the organization have domains with expired or nearly expiring SSL certificates? • Are there suspicious changes in the organization's IP block and A, MX, NS, and other DNS records? • Have there been unauthorized changes in the client's domain registration details recently?
Continuously scan the DNS for threats	• Are there domain impersonation campaigns detected within the past hour? Who is behind these typosquatting domains? • Are there domain generation algorithm (DGA)-enabled resources added or updated within the past hour that could be weaponized? • Do some domains belonging to unsafe categories, such as adult and gambling sites, try to communicate with the client's corporate network? • What domains and subdomains added within the past hour share the same digital footprints (e.g., nameserver, registrant information, SSL certificates, and text strings) as indicators of compromise (IoCs)? What IP addresses do these properties resolve to? • What newly registered or updated domains use self- signed SSL certificates or those issued by less reputable certificate authorities (CAs)? • What endpoints are geolocated in cybercrime hotspots or out-of-service areas?

3. Predictive Threat Intelligence and Actor Disruption

The cybersecurity ecosystem is a rat race between threat actors and security teams, with both parties relying on advanced technologies and highly talented experts. For D&R teams and service providers to win, they have to be proactive and deal with threats before attacks ensue. A complete and well-structured view of the public Internet can help accomplish this, as DNS and domain data is among the first clues of badness.

Notable Use Cases	Connected Data Points
Predict the badness of a domain based on commonalities	• Are there signs of bulk domain registration, such as recurring text strings and the same creation date? Have any of the domains in the group been flagged as malicious? • Does the domain have the same text string as a suspicious typosquatting group? • Does the domain or subdomain share the same IP address as a malicious property? What other cyber resources resolve to the IP address? • Does the domain share the same WHOIS ownership details as the suspicious or malicious domain? What other domains share the same data? • Does the domain have a self-signed or less reputable SSL certificate? What other domains and subdomains use the suspicious or malicious SSL certificate?
Gather information to facilitate the takedown of threat actor infrastructure	• What is the suspicious or malicious domain's registrar? • Who is the malicious domain's registrant? For domains with redacted WHOIS records, what ownership details can be gleaned from their WHOIS history? • To which IP netblock does the malicious IP address belong? Who administers that netblock? • Which CA issued the SSL certificate that figured in an attack?

About Us

WhoisXML API aggregates and delivers comprehensive domain, IP, DNS, and subdomain data repositories. WhoisXML API has more than 52,000 satisfied customers from various sectors and industries, such as cybersecurity, marketing, law enforcement, e-commerce, financial services, and more. Visit whoisxmlapi.com or contact us for more information about our products and capabilities.

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence