Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Enable Deeper and Broader Intelligence-Led Cybercrime Analysis

Challenge

Although seizing domains and websites won't necessarily stop or catch the bad guys, it tells them you have your eyes set on them. But the fact remains that threat actors can easily set up new criminal infrastructure and continue masking their identities on the Web, which makes the work of gathering as many online clues as possible, including real-time and historical Internet events, a never- ending effort.

Data-Driven Solution

At the core of intelligence-led policing (ILP) is information gathering that shapes crime fighting strategies. When it comes to cybercrime, intelligence-led investigations require real-time and historical access to data points connected to digital infrastructure elements, such as hosting service providers, DNS records, IP information, and domain ownership details. These information sources can provide critical clues to help disrupt and unmask perpetrators, uncover crime trends, or prevent online cybercrime in the first place.

Notable Use Cases	Connected Data Points
Early detection and continuous monitoring of counterfeiting domains and sites	• What domains added within the past hour contain the names of legitimate brands? • What other domains share the same current or historical WHOIS information as the cybersquatting domains (e.g., registrant name, organization, email address, and nameserver)? Do they also contain brand names? • What other domains share the same IP addresses as cybersquatting domains? Do they also contain brand names? • What content do the cybersquatting domains host based on screenshot analyses? Are there signs of counterfeiting? • For cybersquatting domains that don't have DNS resolutions or content yet, are there WHOIS data changes that indicate they are being mobilized on a given day?
Broader investigation and early detection of media piracy	• What websites are classified under the Arts & Entertainment category of the Internet Advertising Bureau (IAB)? • Do these websites host content that hint at media piracy, such as offering movie access and music downloads? • What other domains share the same current or historical WHOIS information as the domains (e.g., registrant name, organization, email address, and nameserver)? Do they also host possibly pirated content? • What IP addresses do these websites resolve to? Are there other potentially illicit domains sharing these IP addresses?

Deeper investigation of phishing domains	• What are the phishing domains' WHOIS ownership details? Are there other possible phishing domains sharing the same information? • What mail server did a phishing email use? What other email domains share the same MX record detail? • Is the phishing subdomain part of a legitimate company's infrastructure? If so, have other subdomains been compromised? • Are there vulnerable subdomains under some of the most abused root domains? • To what IP address does the phishing domain resolve? Are there other possible phishing domains hosted on the same IP address? • What SSL certificates did the phishing domain use? What other domains have the same SSL certificate chain details?
Criminal infrastructure takedown	• What organization owns the IP range to which the malicious IP address belongs? What are its contact details? • What are the registrar, registrant, and administrative contact details of a malicious domain or the root domain of a malicious subdomain? • Who issued the malicious websites' SSL certificates? What other clues can you obtain from their SSL certificate chains?

> **WhoisXML API data has led our Cybercrime Unit to clues that greatly contributed to our investigations. We pivot off certain domain and WHOIS data points to see historical domain ownership details, domain connections, DNS resolutions, and other hidden intelligence that could bring us closer to criminal infrastructure takedown, if not case resolution.**
>
> **Investigation Officer**
> **Digital Crimes Unit**

> **We found certain nameservers that were always used for a phishing campaign, having those in our rules enabled us to catch phishing sites before they affected our user base. WhoisXML API is a responsive and reliable provider of domain intelligence. Whenever there are issues, they are quick to respond and resolve them. Working with them is smooth and straightforward.**
>
> **Christine Bejerasco, Senior Analyst**
> **F-Secure Labs**

Finding Your Own DNS Data (FYODD) Doesn't Let You Scale

Delivering a real-time and uninterrupted satellite view of the world's DNS is our core business. The WhoisXML API data engine is built and frequently upgraded to offer you the most complete, updated, and unique Internet intelligence footprints. We aim to contribute to our clients' competitive edge at every step and give back months or years of development cycle time to your most pressing and mission-critical projects and deployments.

How the WXA Data Engine Is Ready to Add to Your Success Today:

1. Collection	2. Unification	3. Maintenance	4. Delivery	5. Innovation
• Internet-wide data sensing and crawling since 2010 • Legal agreements with major data aggregators • Large and growing network of data exchange partners	• Consistent data parsing of multiple data points across formats • Resolving incomplete, conflicting, and inaccurate records	• Addition of new and historical domains, subdomains, and IP and DNS records • Daily updating of millions of WHOIS, DNS, IP, and other records	• Batch feeds and APIs with complete documentation • Different support and customer success tiers • Streaming of domain and DNS data in real-time • Enterprise-grade IT infrastructure	• Ongoing improvement of data coverage, freshness, and accessibility • New features, product iterations, and solutions driven by market demand

Our Crime-Fighting Value Proposition

Our intelligence is available through customized enterprise packages and product suites with multi-year contracts, flexible licensing models, nonrestrictive data access, and dedicated account and customer success teams. Contact us for more information.

Diamond: Includes all products listed below with Premium SLA
Gold: Pick 2 of each Tier, includes Gold SLA
Silver: Pick 1 of each Tier, includes Silver SLA
Starter: Pick 1 Tier-1 product, 1 Tier-2 product

Tier	Product	Update Frequency
P	Real-time & Historic Whois Streaming	Real-time Stream, Daily & Quarterly Feed, Real-time API Lookups
P	Real-time & Historic Passive DNS Coverage	Daily + Weekly Feed, Real-time API Lookups
P	Enterprise & Threat Intelligence APIs	Enterprise APIs T5 & Threat Intelligence APIs (1M CPM)
1	Real-time WHOIS Data Coverage	Daily & Quarterly Feed, Real-time API
1	Real-time DNS Coverage	Weekly Feeds, Real-time API
1	IP Geolocation & Netblocks Data Coverage	Daily Feeds
1	Website Contacts & Categorization Feed	Daily Feed
2	Subdomains Database Feed	Daily Feed
2	IP Netblocks (IPv4 + IPv6)	Daily Feed
2	IP Geolocation Database	Daily Feed
2	Typosquatting Data Feed (Enriched)	Daily Feed
2	Disposable Email Domains Feed	Daily Feed
2	MAC Address Database Feed	Daily Feed

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