Product Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Achieve Superior Coverage of Known Malicious Assets with Our Threat Intelligence Data Feeds

Missed indicators of compromise (IoCs) can blow a hole into your threat intelligence.

Malicious indicators come in many forms and from different sources. Manually collating and processing these web assets daily for blocking can be tedious and time-consuming, and may result in delayed threat response and greater risk exposure if you miss any of them. To catch up with the fast-paced threat landscape, you need daily access to a threat intelligence data feed with extensive coverage of preprocessed and categorized risky assets.

Gain wider threat visibility and ensure faster threat response with ready-made malicious indicator data sets.

Our threat intelligence data feed provides access to 10 files containing different types of web assets that have figured in various malicious attacks and suspicious activities, such as malware distribution, command-and-control (C&C) hosting, botnet operations, phishing campaigns, spam activities, and Tor exit node hosting. Our feeds are updated daily and downloadable in standardized file formats (CSV, JSONL, v4, or HOSTS) for smoother integration. Download file samples or contact us for more information.

Practical Usage

Access daily lists of malicious indicators for:

- **Integration into cybersecurity solutions:** Expand the coverage of your security solutions by adding extensive lists of known IoCs and dangerous assets to your intelligence stack.
- **Stronger network security:** Add our preconfigured deny lists in CIDR notation into firewalls and other network security solutions.
- **Stricter zero-trust policy implementation:** Impose stringent blocking measures to protect networks and systems from malicious resources immediately after detection.
- **Security research and OSINT analysis enrichment:** Use our threat intelligence data feeds to analyze IoCs by threat type and detect cyber threat patterns.

What Threats Do Our Threat Intelligence Data Feeds Cover?

Cyber Attacks	Phishing	Botnets
Malware	C&C Servers	Spam
Suspicious Activities	Tor Exit Nodes	Generic

What Threat Intelligence Data Feeds Are Included?

Our Threat Intelligence Data Feed contains 10 files. See the table below for their brief descriptions.

Data Feed	Description
Malicious IPv4 data feed	Contains known malicious IPv4 addresses that figured in different cyber attacks
Malicious IPv6 data feed	Contains known malicious IPv6 addresses that figured in different cyber attacks
Malicious domain name data feed	Contains known malicious domain names that figured in different cyber attacks
Malicious URL data feed	Contains known malicious URLs that figured in different cyber attacks, along with their hosts
Malicious file hash data feed	Contains known malicious file hashes and the algorithm used to generate them
Hosts files deny list	A deny list containing malicious domains in the hosts file format for immediate blocking
Domains deny list	A plain text file containing domains that should be blocked since they have been detected as active IoCs the previous day
IPv4 deny list	A plain text file containing IPv4 addresses that should be blocked since they have been detected as active IoCs the previous day
IPv6 deny list	A plain text file containing IPv6 addresses that should be blocked since they have been detected as active IoCs the previous day
Nginx compatible IPv4/IPv6 deny lists in CIDR notation	A deny list containing IPv4 and IPv6 ranges in CIDR notation formatted for the ngx_http_access_module

What Threat Intelligence Delivery Models Do You Provide?

Delivery Model	Update Frequency
Threat Intelligence Data Feeds	Daily

About Us

WhoisXML API aggregates and delivers comprehensive domain, IP, DNS, and subdomain data repositories. We have 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 at sales@whoisxmlapi.com for more information about our products and capabilities.

WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence