Widen Your Threat Visibility with Our New Threat Intelligence Data Feeds (TIDF)

Posted on May 11, 2023

In line with our mission of making the Internet safer, WhoisXML API recently launched a new Threat Intelligence Data Feeds (TIDF) offering with the goals of complementing existing security intelligence and systems, widening threat visibility, and accelerating threat response.

“Our Threat Intelligence Data Feeds help achieve superior coverage of known bad web assets. The current cybercrime climate demands extensive threat intelligence to detect malicious events and categorize them into threat types while enabling organizations to act quickly,” says Jonathan Zhang, CEO of WhoisXML API.

Wider Threat Visibility and Faster Threat Response

TIDF is composed of 10 files with distinct intelligence on malicious attacks, namely:

- Malicious IPv4 data feeds
- Malicious IPv6 data feeds
- Malicious domain name data feeds
- Malicious URL data feeds
- Malicious file hash data feeds

- Hosts files deny lists
- Domains deny lists
- IPv4 deny lists
- IPv6 deny lists
- Nginx ngx_http_access_module compatible IPv4/IPv6 deny lists in CIDR notation

These data feeds are available in standardized CSV and JSON file formats, which makes them compatible with most systems. As such, the files can easily and quickly be integrated into existing cybersecurity systems so newly detected malicious indicators are immediately blocked.

Threat Type Classification

Malicious indicators within each file are classified into these types of threats for value-added intelligence useful in deeper analysis and threat attribution:

- **Attack:** Web properties associated with Secure Shell (SSH) brute-force, denial-of-service (DoS), and other cyber attacks.
- **Botnet:** Hosts that are part of a malware-infected network of computers.
- **Command-and-control (C&C):** Web properties seen communicating with botnets and malware controlled by cybercriminals.
- **Malware:** Hostnames, URLs, and file hashes associated with malicious software distribution.
- **Phishing:** Domains, URLs, and hostnames involved in phishing attacks.
- **Spam:** Properties engaged in sending or hosting spam content and messages.
- **Suspicious:** Web properties linked to suspicious activities, such as requesting or scraping huge volumes of data.

- **Tor:** Hosts that serve as Tor exit nodes.
- **Generic:** Malicious indicators that can't be classified into the other threat types above.

TIDF can reinforce cybersecurity solutions with up-to-date threat intelligence, helping security teams and network administrators expand zero-trust policy implementation and strengthen network security. Investigators and security researchers can also glean insights from the data feeds to deepen OSINT analysis and cybercrime investigations.

TIDF files are updated daily, ensuring fresh and relevant information.

We offer flexible pricing and packages to suit your threat intelligence needs.

Want to learn more about Threat Intelligence Data Feeds (TIDF)? Don't hesitate to contact us or download file samples.