BANDURA®

Smart, Simple, Scalable. Everywhere.

Benefits

- Protection from domains and IPs associated with phishing, malware, and spam threats.
- DomainTools Domain and IP Intelligence is automatically updated in Bandura platform ensuring protection is always current.
- Easy and fast deployment via Bandura Cyber Intelligence Marketplace.

BANDURA® + DOMAINTOOLS®

In any online environment, there is the potential for traffic from the protected environment to threat-actor-controlled assets. Connections from trusted users to hostile domains and IP addresses enable malware downloads or command and control, data exfiltration, espionage, and other threat activities. Preventing users from reaching dangerous infrastructure, while simultaneously supporting necessary business functions, is a major component of every network defense strategy. DomainTools DNS Infrastructure Intelligence solutions enable organizations to assess the risk of potentially malicious domains and associated IPs in order to disposition suspicious connections, or even prevent future or real-time attacks.

DomainTools Threat Intelligence

DomainTools DNS Intelligence is driven by the DomainTools Domain Risk Score, which predicts how likely a domain is to be malicious, often before it is weaponized. This can close the window of vulnerability between the time a malicious domain is registered, and when it is observed and reported causing harm.

The Domain Risk Score algorithms analyze a domain's association to known-bad infrastructure, as well as intrinsic properties of the domain that closely resemble those of known phishing, malware, and spam domains. The machine learning behind the Domain Risk Score is the "pre-blocklist blocklist," whereby we alert security technology solutions about high risk domains days, weeks or months before they end up on open source or commercial blacklist of known bad entities.

There are two DomainTools Cyber Intelligence feeds available on the Bandura Cyber Threat Intelligence Marketplace—the DomainTools Domain Hotlist and IP Hotlist.

DomainTools Domain Hotlist

The Domain Hotlist consists of domains that have a DomainTools Risk Score of 99 and higher. These domains are both highly risky and currently active; in other words, operational. This list gives customers a relatively small, easy-to-manage, focused set of domains that they can use to track, monitor, and alert on active malicious domains touching their network.

The Domain Hotlist provides protection from phishing, malware, and spam threats and typically contains over 10 million malicious domains.

BANDURA®

Smart, Simple, Scalable. Everywhere.

DomainTools IP Hotlist

Many of the most dangerous traffic flows in any protected environment are from trusted assets to malicious infrastructure.This makes the population of domains on a hosting IP address an important basis for determining how risky the IP is. The DomainTools IP Hotlist is designed to identify the riskiest population of hosting IP addresses. Two main criteria define this list: the percentage of known malicious and predicted malicious domains hosted on the IP address and the level of traffic it's receiving, as measured in Internet-wide passive DNS collection. The Hotlist is an ideal database for high-confidence block list and detection rule creation. Typical Hotlist size is between 40,000 and 50,000 IP addresses. resolvers, and Tor exit nodes. The feed also includes domains associated with cryptominers.

About DomainTools

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at http://www.domaintools.com or follow us on Twitter:@domaintools

For more information about Bandura's solutions contact us at 1.855.765.4925 ext 3, or by email at sales@banduracyber.com.

www.banduracyber.com