Threat Intelligence

Over 12 Billion Threat Indicators Processed Per Day

Abusix provides threat intelligence for security service providers, government organizations and social networks to discover relevant threats and protect their customers. Using our proprietary sensor networks combined with data from our valued source partners, Abusix provides an unparalleled view of threat resources that enable efficient operation of heuristics engines, automatic detection of compromised sites, zero day detection of new malware variants, hunting of command and control servers, drive by downloads and malware on the web, all allowing for quick identification and remediation of security threats and vulnerabilities.

KEY BENEFITS

100% clean, false-positive free data

Rich metadata allowing you to identify and neutralize malicious content, compromised machines, botnets and bad actors.

Abusix Threat Intelligence Feeds can specifically be tailored for your organization's use-case

Get the same data set used by major security providers as well as Virus Bulletin and other security rating services to rank and evaluate security vendors

TRUSTED BY:

Clarivate Analytics

SOPHOS

CYREN

TREND MICRO

accenture

FORTINET

Avira

LinkedIn

Threat Intelligence Data is Power

To anticipate and respond to sophisticated cyber-attacks, organizations need to understand attacker motivations, intentions, characteristics, and methods.

FOR SECURITY VENDORS

'Get the same data set used by major security providers as well as Virus Bulletin and other security rating services to rank and evaluate security vendors, with Abusix'

Security vendors need to constantly tune their security heuristics engines in real-time, to address zero day malware and MS-born threats, analyze malicious code and track ransomware command and control servers, every second of every day to catch the latest shape shifting threats.

Abusix' threat intelligence feed provides a constant corpus of data enabling security vendors to detect new email borne malware, phishing attacks and botnets. With Abusix' threat intelligence feeds, Security Providers receive message streams based upon country of origin, language, mime types, mime character sets, key-word expressions etc. for hunting malicious actors, phishing and drive by downloads.

FOR GOVERNMENT AGENCIES

'100% pure spam and false positive free. Use the data with confidence in your automated country CERT and law enforcement workflows.'

Access to timely cyber threat intelligence is a critical defense strategy in any dynamic cyber threat landscape. Government agencies need as much external data about suspicious and malicious activity in their system as possible to successfully collect good legal evidence and even verify the identity and location of the cyber-criminal.

Abusix' filtered country feed provides a constant real-time flow of criminal exploits. Abusix threat intelligence enables government agencies to detect, analyze, understand and prosecute offenders that operate within their country's boundaries.

FOR SOCIAL NETWORKS AND PREMIUM BRANDS

‘Quickly see new malicious actors hosting branded trademarks and copyrighted images, as well as locate malicious sites hosting downloads that are ready to infect customers and spy on their activity.’

Brands and Social Networks need to be proactive in order to prevent spoofing and phishing exploits before significant damage is done.

Abusix’ IP/domain list and filtered key message feed enables brands to mitigate abuse and fraud by allowing them to see threats based on expressions such as brand, domain, and cousin names, as well as campaign expressions and their variants.

KASPERSKY lab

“The cooperation with Abusix has been wonderful. Using Abusix Data Services as our data source, Kaspersky Linux Mail Security 8.0 won the VBSpam+ award in the latest Virus Bulletin with a detection rate of 99.75% and zero false positives.
That is awesome.”

Kaspersky Labs

Contact us to learn more about
Abusix Threat Intelligence Feeds.

sales@abusix.com | +1 (855) 522-8749 | www.abusix.com