Abusix Threat Intelligence Datasheet

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

GET MORE DATA FROM MORE SOURCES...

Abusix Threat Reporting provides a constant corpus of threat rich data allowing you to:

- Identify spam in your filters
- Identify malicious files
- Identify compromised machines and botnets
- Identify malicious or poorly managed networks
- Identify malicious URLs
- Identify malicious actors
- Identify bad senders

GET MORE OF WHAT YOU REALLY NEED...

- Receive and choose the volume of messages from the same corpus as Virus Bulletin, specifically designed for tuning Antispam filters.
- A message feed filtered for further tuning, based on your requirements such as language, region, filetypes, etc.

KEEP YOUR USERS SAFER...

- 100% false positive free, allowing customers to use the data automatically.
- Network Abuse Feeds are specifically tailored for ISPs, hosting providers, email service providers and CRM companies who need additional insight into subscribers who are abusing their services.

THREAT INTELLIGENCE SERVICES

SPAM THREAT INTELLIGENCE

Anti-spam vendors need to constantly tune their spam heuristics engines to catch the latest shape shifting threats.

Abusix's Spam Threat Intelligence service is a real-time corpus of spam messages. This feed may be used for tuning your anti-spam filters, and monitoring your network or services for bad actors and compromised systems.

For security providers, this is the best solution in the marketplace today, as it provides you with the same data set used by major security providers as well as Virus Bulletin to rank and evaluate providers.

For network and service operators, this is the best solution in the marketplace today, as you are able to see the start, peak and end of spam runs that will get your IP addresses blacklisted.

This feed is 100% pure spam, false positive free, allowing you to use the data with confidence in your automated workflows.

MALICIOUS FILE THREAT INTELLIGENCE

Abusix's Malicious File Threat Intelligence service is a real-time corpus of files derived from the 400+ million spam messages Abusix processes each day.

Security vendors need to keep their virus outbreak filters current in real-time to address zero day malware and MS-born threats, analyze malicious code, and track down ransomware command and control servers by opening the payloads in sandboxes, every second of every day.

Service providers need to gain access to the latest malicious email borne payloads. This feed is a must have, to complete the suite of file feeds you use to hunt for threats.

URL THREAT INTELLIGENCE

Security and Brand Protection vendors of all types need to constantly hunt for new websites and webpages that are spoofing and phishing brands and users generically, hosting drive-by download or malware threats, and phish kits or crimeware.

Abusix's Malicious URL Threat Intelligence service is a constant real-time raw stream of all URLs Abusix sees in 400+ million per day black and grey spam message streams. This feed is a must have, to complete the suite of data feeds you use to hunt for threats.

This feed allows you to 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.

ABUSIX THREAT INTELLIGENCE FEATURES

The depth and versatility of Abusix's Threat Intelligence Feeds make the data a valuable and critical component of the cyber defences deployed by security vendors, network service operators and social networks, government agencies, large enterprises, and researchers.

MESSAGE FEEDS

Raw Message Feeds

Receive 100% pure spam messages.

Filtered Message Feeds

Receive 100% pure spam messages, filtered by your selected attributes.

Messages filtered on any or all of the following in the headers:

- Source by region, country, asn, cidr, IP address or other
- Transaction method (eg: SMTP or ESMTP)
- Internet protocol (eg: IPv4 or IPv6)
- Other

1

Messages filtered on any or all of the following information in the transaction, headers, and body:

- Domains, keywords, expressions
- HTML
- Mime character types
- CName
- CName IP location
- Attachment mime types
- Other

2

Use Cases

Abusix Threat Data customers use our feeds for a wide range of purposes, including the following:

Security Anti Spam Heuristics	**Security vendors need to train and tune filters each day, all day.** Abusix' spamfeed provides a constant corpus for training filters, detecting compromised systems, bad actors in your network, new email borne malware, phishing attacks and botnets. Abusix' FILTERED spamfeed, applied after the raw feed allows Security Providers to receive focused message streams based upon mime types, mime character sets, keyword expressions, and country of origin.

Network / Service Operators and Providers Access, Hosting, Email Service Providers and Social Networks	**Network owners and large enterprises need to know when botnet IPs are active behind their DMZ to track potential threats coming onto their networks such as spam runs occurring that can cause blacklistings and other damage so that they can shut down the bad actors and compromised machines as quickly as possible.** Abusix' FILTERED net message feed for your network range provides you with an early warning of a bad actor or outbreak and an unparalled view to your blindspots.
Country CERT, Law Enforcement, and TLD Registries	**CERT organizations, law enforcement, and TLD Registries need to keep watch for criminal activity, threats of national interest, spam, and abuse coming from its country and top level domain.** Abusix' FILTERED country feed provides a constant, real-time flow of criminal exploits. Abusix enables country CERTs and law enforcement to detect, analyze, understand, and prosecute offenders that operate within their country's boundaries.
Brand Protection Providers, Social Networks and Government Agencies	**Brands, social networks, and government agencies are spoofed and phished every day. Many of these entities see social engineering hacks, fraud, and phishing late in their lifecycle or sometimes not at all. Abusix allows companies, governments, brand protection teams and market intelligence services to monitor phishing and abuse.** Abusix' FILTERED keyword or CName feed allows you to mitigate abuse and fraud by allowing you to see threats based on expressions such as brand, domain and cousin names, as well as campaign expressions and their variants.

Specifications

1. You will receive messages that are 100% clean and fresh spam, with NO Ham.
2. The original spam message in its entirety, as caught by the Abusix spam traps, will arrive just a few moments after we have received it.
3. The feed may be filtered to your use-case; thus, designed to provide you with the information you need to maximize protection.

Format	RFC 6650 (MARF)
Data	All RFC 822 headers, the body of the email and attachments if applicable.
Delivery Method	SMTP, AWS S3, SFTP, STOMP, or other transport upon demand.

Requirements

- Let Abusix know if you prefer a raw random or filtered message feed.
- Provide Abusix with a non-filtered recipient email address, AWS S3, SFTP, Stream or other transport instructions.

MALICIOUS FILES

File Feeds

- This is a feed of all the files without messages we see in spam, on a daily basis, deduplicated.

Filtered Message Feeds

- This is a randomly selected message feed of 100,000 messages per day; filtered by mime types that you select and care about the most.

Use Cases

Security ZeroDay Outbreak Protection	**Anti-Spam and Anti-Malware vendors need to be on the alert for ZeroDay malware attacks and MS Office-born threats every second of every day.** Abusix' file feed is derived from our black and grey spam feeds and provides a constant corpus of files designated as safe to block.
Ransomware Hunting	**Security vendors need to hunt for ransomware command and control servers.** Abusix provides a constant corpus of files for sandboxing, detonating, and hunting for ransomware and other command control servers.
Malware Research	**Anti-Virus researchers need a corpus of fresh files to hunt for new variants of malware.** Abusix file feed is ideal to build a library of files to look for viruses and MS Office malware variants.

Specifications

1. Abusix will provide you the files Abusix sees, within the sources you select.
2. All files are found in spam and are thus 100% safe to block.
3. The file feed will be filtered to your use-case, designed to provide you and your customers the information you need to maximize protection.

Format	Individual files or messages
Data	• If "all files" is selected, only files are delivered. • If "Messages with Files" is selected, all RFC 822 headers, the body of the emails and all attachments are delivered.
Delivery Method	AWS S3, SFTP, SMTP, STOMP or other transport upon demand.

Requirements

- Let Abusix know if you would prefer a file or filtered message feed.
- Provide Abusix with a non-filtered recipient email address, AWS S3, SFTP or Stream instructions.

AGGREGATE REPORTING

URL Feeds

Receive a feed of all the URLs that we see in spam.

IP Domain Feeds

Receive a feed of all the sender IP/Domain pairs we see in spam.

Use Cases

Security Malicious Site Hunting	**Security vendors need to constantly hunt for malicious actors.** Abusix' URL reporting contains all URLs found in our black and grey spam feeds providing a constant corpus for hunting for malicious actors hosting phishing and driveby downloads.
Email Providers	**Email providers need as much external data about prospects and new users in their system as spam runs cause blacklistings and damage email provider IP reputation.** Abusix' IP/domain reporting and netfeed provides email providers with an unparalleled view to your blind spots to bad actors in your network and provide you with forewarning of blacklistings.
Social Networks, Premium Brands and their Brand Brand Protection Providers	**Often brands see fraud and phishing late in their lifecycle or not at all. Brands need a better way to be on the lookout for social engineering attacks to prevent spoofing and phishing exploits.** Abusix' URL reporting provides raw threat data alerts in real-time to allow you to prevent brand abuse and fraud. In addition, Abusix' spam message feeds allow you to see known to see threats in even greater detail, based on brand, domain and cousin names, as well as campaign tag lines.
Security Solution Vendors, Access and Hosting Providers	**Security vendors and networks need to constantly watch for bots and malicious actors.** Abusix' IP/Domain pair reporting identifies malicious actors and botnets in your network.

Specifications

1. Abusix will provide you with specific metadata elements, as seen within the sources you select.
2. All meta data elements are found in spam and are thus target rich.
3. The data may be filtered to your use case, by geography, language, region, network range; and thus, designed to provide you and your customers the information you need to maximize protection.

Format	Hourly reports or streamed
Data	Elements selected.
Delivery Method	AWS S3, SFTP, STOMP or other transport upon demand.

Requirements

- Let Abusix know if you would prefer a url or IP/Domain feed.
- Provide Abusix with AWS S3, SFTP or Stream instructions.

ABOUT ABUSIX

Based in Silicon Valley, with operations in Karlsruhe, Germany; Abusix has long been considered one of the world's leading authorities on tracking and solving network threats. Abusix threat intelligence data services provide 100% clean, real-time, global threat data to more than 70+ customers including AV Comparatives, AV Test, NSS Labs, Virus Bulletin, Accenture iDefense, Clarivate Analytics MarkMonitor, Avira, Proofpoint, Cloudmark, Cyren, ESET, McAfee, Sophos, Trend Micro and others.

Contact us to learn more about
Abusix Threat Intelligence

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