Enterprise Threat Data Feeds

Malware Patrol

NO SINGLE VENDOR CAN PROTECT FROM ALL CYBER THREATS.

The stakes are higher than ever and your company's data is its most valuable asset. The safest, most logical plan for your organization is to obtain threat intelligence from multiple sources and utilize it as part of a layered security strategy.
Since 2005, Malware Patrol focuses exclusively on malware indicators. Crawling systems, along with an active open source community and industry partnerships, maintain our malware data sets current and geographically diverse.

ACCURATE, FOCUSED DATA:
Millions of malware and ransomware indicators of compromise and meta data.

UP-TO-THE-MINUTE PROTECTION:
Updates every hour offer protection from the latest cyber threats.

EASY TO USE & INTEGRATE:
Customizable data feed contents and format, compatible with the most popular security systems.

MALWARE PATROL THREAT DATA FEEDS

Malware & Ransomware URLs: Sites actively hosting malware and ransomware.

C&Cs: URLs of command and control systems used to relay stolen financial information.

IP Addresses: currently hosting malicious binaries, C&Cs and DGAs.

Malware hashes: MD5 and SHA-1 hashes of malware binaries currently available on the net.

DGAs: Domain names generated via DGAs used by malware and ransomware to contact C&Cs.

Real Time DDoS Attacks

DDoS attacks are a major threat to companies of all sizes. Apart from implementing DDoS mitigation strategies, access to threat data about the latest attacks is vital to understand the current landscape and its trends.

Malware Patrol maintains a data feed containing live records of amplification and reflection DDoS attacks. It is produced with data collected by sensors deployed all over the Internet. The feed is updated every 20 minutes.

OUR DATA FEEDS PREVENT ACCESS TO MLLIONS OF MALICIOUS URLS, C&Cs AND IP ADDRESSES

Prevent malware infections

End users won't access URLs that download malware or be redirected to other malicious sites

Prevent data loss and ransom demands

Avoid ransomware that encrypts your users' files and demands payment for release

Stop data transmission to remote servers

Data and files won't be transferred to C&C servers when access to them is blocked

FREE
Feed Evaluation Available

Contact us to inquire about data feed customization to meet your business and system requirements. We are happy to arrange discounts for bundled feeds and multi-year payments

commercial@malwarepatrol.net

Enterprise Threat Data Feeds

Malware Patrol

MALWARE URLS

- Plain text or custom formatted.
- updated every hour
- Contents: protocol, full domain name, parent directories and malware file name*
- Downloadable via HTTPS (requires user authentication)
- MD5 and SHA-1 hashes of the feed for integrity validation

CUSTOM DATA FEEDS

- Customizable content and format.
- Pre-formatted options available to the popular security systems: CIF, XML, CSV, JSON, SpamAssassin, Squid, ClamAV
- Our intent is to simplify the process of consuming data
- Feeds also available at Check Point ThreatCloud IntelliStore

IP ADDRESSES OF SERVERS HOSTING MALWARE BINARIES, C&CS AND DGA DOMAINS

Updated every hour
Plain text a custom formatted including the following fields:

- MBL ID (for reference only)
- IP address
- Type: malware, C&C or domain generated via DGA
- Malware, C&C or family classification
- Detection timestamp

Downloadable via HTTPS (requires user authentication), MD5 and SHA-1 hashes of the feeds for integrity validation

MALWARE/SUSPECT SAMPLES (BINARIES)

Samples are distributed to clients upon discovery by our system
Distribution according to customer's needs (AWS S3, FTP upload, HTTP POST, etc.)
Samples are compressed and password protected
Text file is included in the sample archive containing the following information:

- MBL ID (for reference only)
- Sample classification
- Sample MD5 and SHA-1 hashes

MALWARE/SUSPECT SAMPLE HASHES

Updated every hour
Plain text or custom formatted including the following fields:

- MBL ID (for reference only)
- Sample MD5 and SHA-1 hashes
- Sample classification
- Detection timestamp

Downloadable via HTTPS (requires user authentication)
MD5 and SHA-1 hashes of the feed for integrity validation

DGA DOMAINS

Updated every day. Contains domain names generated via DGA for the current day, the day before and the one after, therefore providing coverage to all time zones
Plain text or custom formatted including the following fields:

- Domain name (day before, current day and next day)
- Registration flag (domain registered or not)
- Registration timestamp (if applicable and available)
- Registrar (if applicable and available)
- Name server(s) (if applicable and available)
- IP address(es) hosting the domain (if applicable and available)

- Download via HTTPS - requires authentication
- MD5 and SHA-1 hashes for integrity validation

FREE
Feed Evaluation Available

Contact us to inquire about data feed customization to meet your business and system requirements. We are happy to arrange discounts for bundled feeds and multi-year payments

commercial@malwarepatrol.net