Malware Patrol

STOP CYBERATTACKS BEFORE THEY STOP YOUR BUSINESS

Cybersecurity teams and researchers around the world rely on Malware Patrol's timely and actionable data to expand their threat landscape visibility and to improve detection rates and response times.

We offer a variety of IoCs related to the most prevalent attack vectors in formats compatible with popular industry security tools and platforms.

Our systems verify each IoC every day to ensure that our feeds contain only active threats.

Data feeds are available individually or in packages, according to your needs.

PREVENT, DETECT, AND CORRELATE CYBER ATTACKS

- Free data evaluation and technical consultation
- Hourly updates
- No download limits
- Free customization to your ingestion requirements
- Dedicated, easy-to-reach US-based tech support
- Simple pricing with an unlimited-use commercial license
- Significant discounts for bundles and multi-year subscriptions

- Support numerous security and intelligence use cases such as NOC/SOC, SIEM/SOAR, threat hunting, IDS/IPS, campaign tracking, incident response, and more.
- Automatically operationalize high confidence, timely and contextualized Indicators of Compromise (IoCs) in your environment.
- Gain early insight and operational knowledge of the latest crimeware campaigns.
- Ease integration with security products and services.
- Malicious file and network-based indicators associated tactics and techniques (MITRE ATT&CK)

commercial@malwarepatrol.net

GET ONLY WHAT YOU NEED BUILD YOUR OWN FEED

We can create a feed that works for your organization - in most cases at no cost. Common customization requests include:

- Add context / metadata
- Whitelist / remove specific domains
- Create an entirely new feed - our team enjoys a challenge
- Combine multiple feeds
- Remove fields or change format

WE INTEGRATE WITH YOUR ENVIRONMENT

MISP Threat Sharing, THREATBLOCKR, MikroTik, FORTINET, CISCO, ANOMALI, THREATQUOTIENT, ClamAV, SURICATA, CARBON BLACK, DNS BIND, pfSense, POSTFIX, SquidGuard

Thousands now use the indicators of compromise (IoCs) collected by Malware Patrol to protect networks and assets in more than 175 countries

commercial@malwarepatrol.net

Bitcoin Transactions

The Bitcoin Blockchain Strings contains all the text from the blockchain since its inception. This often includes information like URLs that point to obscure/illegal websites, encoded files, and malicious source code. Updated every 6 hours.

The Bitcoin Transactions includes easy-to-parse information on all block transactions since the genesis block on January 3, 2009. An average of 50,000 transactions happen every day. A JSON file is produced for each transaction, as soon information is available.

C2 Address + MITRE ATT&CK

Most malware and ransomware families implement communication with a C2 system that is responsible for relaying stolen information or downloading additional payloads. Use these addresses to block access, create alerts on an IDS/IPS system, or investigate communications between samples and C2s. This feed covers over a hundred families. Correlated with MITRE ATT&CK to include the malware family's TTPs and groups. Updated every hour.

Cryptomining Cryptojacking

The sites in this feed load JavaScript which uses the visitor's CPU to mine cryptocurrency. This data feed is available for free to our Enterprise customers. An extra JASON file is provided that contains code snippets detected on the sites. Updated twice daily.

DDoS Attacks (Real-Time)

Many systems and protocols widely available on the internet are abused by attackers to generate abnormal amounts of traffic, including NTP, DNS, CharGEN, SSDP, among others. This feed contains live records showing the victims of amplification and reflection DDoS attacks that have happened in the last 24 hours.

DNS-over-HTTPS (DoH) Servers

This feed contains known DNS-over-HTTPS (DoH) servers. DoH allows users to bypass the DNS-level controls put in place to protect your network against known threats. This feed is to help security teams control/monitor the use of DoH in their environment. Updated every hour.

DNS RPZ Firewall

RPZ (Response Policy Zone) functions as a DNS firewall in which rules are expressed in specially constructed zone files. This provides a granular method of leveraging threat data for the detection and prevention of malware and ransomware activities at the DNS level.

We offer seven separate RPZ zone files: (1) C2s, (2) Cryptominers, (3) DGAs, (4) DNS-over-HTTPS servers, (5) Malware, (6)Newly registered COVID-related domains, and (7) Phishing sites. Updated every hour.

Domain Names Generated via DGAs

We monitor domain generation algorithms (DGAs) used by dozens of malware and ransomware families. Blocking access to these domains is an effective way to prevent data loss and extortion because most ransomware will not be able to encrypt files if it can not reach a C2 server to retrieve cryptographic keys. Monitoring network traffic to such domains is also a way to locate internal network computers that may be infected. Updated every hour.

High Risk IPs

Addresses involved in a range of malicious activities, such as spam, break-in attempts, malware distribution, botnets, and command-and-control communications. Data is collected from Malware Patrol's network of honeypots and trusted third-party sources.

commercial@malwarepatrol.net

Malicious Domains

The feed includes domains actively involved in malicious activities. The data is derived from five of our Enterprise feeds: Anti-mining, Comand-and-Control (C2) Addresses, DGAs, Malware & Ransomware URLs, and Phishing. Monitoring traffic destined to these sites, as well as potentially blocking access, is an effective network protection measure. Updated every hour.

Malicious IPs

IP addresses known to actively host malicious files and C2s systems for malware and ransomware. Monitoring traffic destined to such addresses, as well as potentially blocking access to the ones that host C2s, for example, is an effective network protection measure and provides valuable information for research purposes. Updated every hour.

Malware & Ransomware URLs

This feed contains URLs currently hosting malware and ransomware. There are two formats: (1) Sanitized, which includes protocol, hostname, domain name, directories (2) Unsanitized, which includes protocol, hostname, domain name, directories, file name, and extensions of the malware. The unsanitized feed is preferable when downloading the malware is important. Updated every hour.

Newly Registered Domains

On average, 175,000 new domains are registered every day, with many intended for malicious purposes. This feed contains records of new domains registered on a specific day, including DNS resolution of the most useful records. To add context, the data is correlated with IoCs from our other feeds, and DNS is resolved. Updated every hour.

Malware Binaries or Hashes

Samples are collected around the internet and analyzed by our internal system and multiple anti-virus products. If no malware is detected, our automated engines analyze the binary to determine its potential to be a new (unclassified) sample.

The Malware Binaries (Sample) feed contains malicious binaries currently available on the internet, shared immediately after categorization. Unpacked samples are also available. Updated every hour.

The Malware Hashes feed contains MD5 and SHA-1 hashes of malware and ransomware samples currently available on the internet. Updated every hour.

Phishing

Phishing remains one of the top cyber menaces, accounting for 90% of data breaches. We collect phishing URLs from a variety of sources, ensuring coverage of the most current campaigns. A human review process increases accuracy.

Add on: For machine learning/AI tool purposes, we offer a database of phishing website screenshots (JPEG), accompanied by perceptual hashing data on the images. Updated every hour.

Risk Indicators

A variety of threat-related IoCs, including: MD5, SHA1, and SHA256 hashes, email addresses, cryptocurrency addresses, and CVEs. Data is collected from trusted third-party sources.

TOR Exit Nodes

Addresses of active Tor exit nodes as reported by the Tor Project. Frequently involved in malicious activities, it is advisable to monitor, if not block, traffic from these IPs.

commercial@malwarepatrol.net