INTELLIGENT THREAT DATA

Malware
Patrol

Malware • Ransomware • Phishing

PREVENT, DETECT, AND CORRELATE CYBER ATTACKS

ABOUT US

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

We offer a variety of IoCs from the latest malicious campaigns, all of which are verified each day to ensure that our feeds contain only active threats.

FEATURES

- Free data evaluation
- Hourly updates & no download limits
- Free customization to your ingestion requirements
- Dedicated, easy-to-reach US-based tech support
- Simple, business-friendly pricing and licensing
- Discounts for bundles and multi-year subscriptions

DATA FEEDS

- Bitcoin Transactions
- C2 Servers + MITRE ATT&CK
- Cryptojacking
- DNS-over-HTTPS (DoH) Resolvers
- DNS RPZ Firewall
- Domain Names Generated via DGA
- Intrusion Insights
- Malicious Domains
- Malicious IPs
- Malware & Ransomware URLs
- Malware Binaries or Hashes
- Newly Registered Domains
- Phishing URLs, screenshots, & HTML
- Risk Indicators / OSINT Data
- Scam Domains by ScamAdviser

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

The indicators of compromise (IoCs) collected by Malware Patrol are now used by thousands to protect networks and assets in more than 175 countries.

INTEGRATIONS

Malware Patrol offers machine-readable threat intelligence (MRTI) in formats that work with many of the industry's most popular cyber security tools and platforms. This way, companies can protect themselves using our reliable, historically rich data without needing additional resources to do so.

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.

Command & Control (C2) Servers + 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. 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.

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) DoH servers, (5) Malware, (6) Geo-political NRDs, 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 malware will not be able to move through the cyber kill chain (download additional payloads, exfiltrate data, encrypt files) if it cannot reach a C2 server. Monitoring network traffic to such domains is also a way to locate internal network computers that may be infected. Updated every hour.

Intrusion Insights

We deploy honeypots across the globe to mimic a range of services and devices. Attacks against these tools provide real-time visibility into the targets and tactics of malicious actors. Armed with this knowledge, organizations can prioritize and allocate their resources more effectively, focusing on the most prevalent attack vectors and vulnerable systems. Updated every fifteen minutes.

Malicious Domains

The feed includes domains actively involved in malicious activities. The data is derived from five of our Enterprise feeds: C2 Servers, Cryptomining, DGAs, Malware & Ransomware URLs, and Phishing. 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.

Malware Binaries or Hashes

The Malware Binaries feed contains malicious binaries currently available on the internet, shared immediately after categorization. Unpacked samples are also available. The Malware Hashes feed contains MD5 and SHA-1 hashes of malware and ransomware samples. 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.

Phishing

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.

Scam Domains by ScamAdviser

Domains related to online shopping, investment and crypto, identity theft, advance fees, employment, romance, subscriptions, and other types of scams. Updated every hour.

FREE OSINT Feeds (3)

High Risk IPs

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

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 Node IPs

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.

Incident Response

Incident Analysis

Threat Hunting

IDS • IPS

DNS Firewall

SIEM • TIP • SOAR

STOP THREATS BEFORE THEY STOP YOUR BUSINESS

REQUEST YOUR EVALUATION

www.malwarepatrol.net

commercial@malwarepatrol.net
+1.813.321.0987
+55.11.3042.2444