threater

Malware Patrol

SMART, SIMPLE,
SCALABLE.
EVERYWHERE.

Security professionals tasked with protecting assets against malicious actors rely on cyber threat intelligence from external sources to expand their team's threat landscape visibility. Using indicators related to current threats, security teams can correlate, detect and prevent cyber attacks aimed at their organizations.

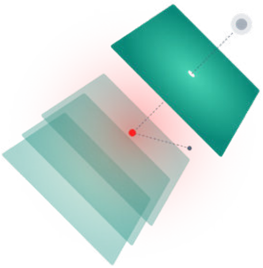
According to a study conducted by the Ponemon Institute:

78%	of respondents rate the importance of threat intelligence in achieving a strong cyber security posture as very high
46%	of respondents believe commercial data feeds provide more actionable intelligence than free sources

Malware Patrol specializes in real-time threat intelligence that protects enterprise users and valuable assets. The highly refined and continuously updated indicators identify malware/ ransomware samples and distribution points, command and control (C2) servers, phishing sites, DGAs, crypto-miners and other threats.

Benefits

- Better protect your network from malware and ransomware, as well as communication with their control infrastructures (C2s, DGAs, Tor).
- Prevent access to phishing sites, the most common attack vector and a popular delivery mechanism for ransomware.
- Maintain control over DNS resolutions by blocking access to DoH servers.
- Malware Patrol Threat Intelligence automatically updated in Threater platform ensuring protection is always current.
- Easy and fast deployment via Threater Cyber Intelligence Marketplace.



Malware Patrol Threat Intelligence

Collecting, analyzing and monitoring threat indicators since 2005, Malware Patrol has developed an extensive network of global sensors, along with other proprietary data collection and identification mechanisms. Both automated and human analysis processes are used to verify and prioritize the data. The result is a vast database of unique and historically rich – "intelligent" – threat data.

Malware Patrol's automated systems verify each indicator daily to ensure that its feeds contain only high confidence data. Feeds are updated hourly with newly found threats. Use these feeds to increase your visibility of active threats and to block malicious and unwanted traffic to/from your network.

Malware Patrol + Threater

Malware Patrol has two subscription offerings available on the Threater Threat Intelligence Data Marketplace. Malware Patrol Essentials is an IPv4 Deny List that includes addresses associated with malware, ransomware, C2 servers, and Domain Generation Algorithm (DGA) infrastructure. Malware Patrol Enterprise is both an IPv4 and Domain Deny List and includes an expanded set of indicators. The Malware Patrol Enterprise feed includes IP and domain indicators associated with malware, ransomware, C2 servers, DGA infrastructure, phishing, DNS-over-HTTPs (DoH) resolvers, and Tor exit nodes. The feed also includes domains associated with cryptominers.

About Malware Patrol

Malware Patrol is a boutique threat intelligence company. All resources go into making sure the data produced is of the highest quality possible. Malware Patrol's proprietary systems work non-stop to collect and validate IoCs, the result of which is timely intelligence that allows customers to confidently detect, correlate, and prevent cyberattacks. Founded in 2005, Malware Patrol's historically rich database is derived from geographically diverse sources and used by managed security service providers (MSSPs), enterprises, and cybersecurity teams to protect users, networks and assets in more than 175 countries. For more information visit malwarepatrol.net.