ANOMALI®

Malware Patrol

INTELLIGENT THREAT DATA

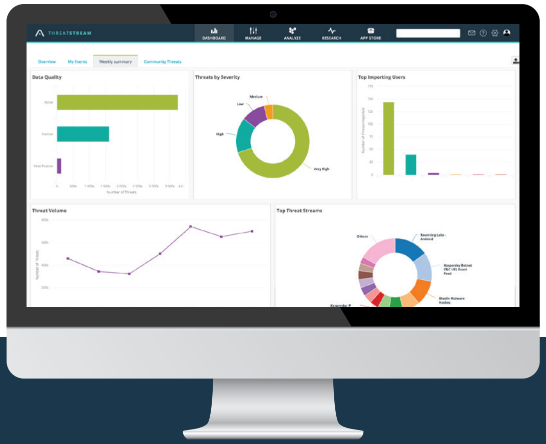
Detect and respond to the latest cyber threats with Anomali and Malware Patrol

MALWARE PATROL AND ANOMALI JOINT SOLUTION FEATURES:

- The Anomali Threat Platform connects up-to-the-minute IOC data feeds from Malware Patrol with your existing security solutions, making the detection and response to threats faster and more accurate
- Access to Malware Patrol's historically rich data, covering threats dating back to 2005
- High-confidence indicators allow you to automate security actions saving time and resources, all while blocking validated, active threats

IMMEDIATE TIME TO VALUE

- Leverage existing cybersecurity investments with up-to-date and accurate threat data
- Focus scarce resources and make decisions based on vetted indicators
- Instant coverage against the latest cyber threats



INTELLIGENT THREAT DATA

Organizations tasked with protecting assets against malicious actors rely on indicators of compromise (IOCs) from external sources to improve their team's threat visibility and prioritization. Anomali and Malware Patrol join forces to provide vetted, actionable threat intelligence feeds that protect your customers and networks against phishing, malware, ransomware, data exfiltration, and brand infringement, among other cyber threats.

CUSTOMIZED INTELLIGENCE

Data feeds tailored to protect from threats that affect your company

ACCURATE & ACTIONABLE

Trustworthy indicators for confident decision making

IMMEDIATE RESULTS

Instant activation, immediate coverage, constant updates

CASE STUDY

CHALLENGE:

Phishing remains one of the top cyber menaces accounting for 90% of data breaches. Methods used by attackers continue to improve and evolve. This makes staying ahead of attackers a constant challenge. Protecting against phishing threats is a basic - and crucial - requirement for businesses of all sizes.

SOLUTION:

Malware Patrol collects phishing data from a wide variety of sources – crawlers, emails, spam pots and more – to ensure coverage of the most current campaigns. Our data undergoes both machine and human analysis, resulting in a higher detection rate of campaigns that use lesser known attack methods. We also offer phishing website screenshots along with perceptual hashing that can be used to train AI/ML models.

CUSTOMER BENEFIT:

Reduce the number of successful phishing attacks against your customers/organization. Optimize resources with vetted low-noise threat data. Use perceptual hashes to train systems to recognize undetected phishing attempts. A combination of screenshots and metadata can be used to track and/or correlate campaigns and educate end users.

CASE STUDY

CHALLENGE:

Preventing malware and ransomware infections is an important and extremely complex task. Criminals use a variety of attack vectors, including zero days, social engineering and known vulnerabilities, to ensure weaknesses are exploited. Cybersecurity teams have double the work of their attackers: they must manage their organization's attack surface while keeping abreast of the techniques being used so they can spot and block attackers.

SOLUTION:

While recognizing every attempt to infiltrate your network might not be feasible, protecting against the widest possible range of attack vectors is. Malware Patrol offers indicators of compromise that cover currently employed malware TTPs, including URLs, hashes, C2s, DGAs, IPs and newly registered domains. Together, these feeds create a multi-faceted defense against threats.

CUSTOMER BENEFIT:

Protect your customers and networks against the latest cyber threats, including phishing, malware, ransomware, data exfiltration, and brand infringement with data feeds customized to your needs and environment.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®