

Know Your Exposure to Advanced Threats with Dynamic Malware Analysis

ThreatAnalyzer is the industry's only malware analysis solution that enables you to completely and accurately quantify the risk and exposure your organization faces from any malware threat.

ThreatAnalyzer enables you to recreate your entire application stack (including virtual and native environments) in which you can detonate malicious code to see exactly how malware will behave across all your network and systems configurations.

Within minutes of detonating a malware sample, you will know exactly which system configurations on your network are vulnerable to any threat, enabling you to instantly respond by isolating systems and implementing defenses to prevent infections.

Bolster Your Defense Against APT's, Targeted Attacks and Zero-Days

Proactively root out advanced threats and defend against data-breaching malware in three steps:



Automate

Quickly recreate events and reduce malware analysis times from hours to minutes. Exponentially grow the number of malware samples you process every day, and eliminate the time-consuming, expensive and error-prone manual analysis that leaves you vulnerable to advanced cyber threats.



Analyze

Understand the nature of each threat targeting your network. In-depth behavioral analysis across your entire application stack shows you how malware executes, changes made to your systems, any network traffic generated, applications exploited and what data is targeted.



Act

Real-time intelligence to block and remediate threats and improve response times. Immediately begin blocking threats, alerting team members and remediating threats from your network with confidence that malicious code is removed and system changes are corrected.

Are you prepared for today's advanced threats?

250,000 new malware samples created every day

40% of data breaches involve malware

47% of enterprises do not use malware analysis tools

Quickly identify data-breaching malware with ThreatAnalyzer.

Recreate all of your 32- and 64-bit system configurations to know how malware will behave across your entire application stack.

Create your own Malware Determination Rules to alert you to the malicious system activity that concerns you most.

Correlate discovered malware and malicious behavior with known threats like bad URLs with integrated threat intelligence.

Leverage indicators of compromise and fuzzy hashing to identify malware variants used by threat actors to evade detection.

Identify and Remediate Advanced Malware Threats

ThreatAnalyzer runs files and URLs in a monitored environment to analyze and determine potential risks. The solution automates behavior analysis to identify APTs, targeted attacks, Zero-day threats and other sophisticated malware through:

Customizable Environments

Analysis across all system configurations: Mimic your environment and run in a customizable native or virtual environment so you know how samples will affect your network and application stack.

64-bit and 32-bit Microsoft Windows platforms: Recreate all your 32- and 64-bit operating system environments, including WoW64 (Windows 32-bit on Windows 64-bit) for more in-depth and versatile analysis.

Fuzzy hashing: SSdeep metrics enable you to quickly identify any resemblance of unknown or like malware variants saving time and unmasking sustained attacks.

Custom Malware Determination Rules: Create your own rule sets to ensure that the malicious behavior that concerns you most is a component of all malware analysis, quickly alerting you to new threats.

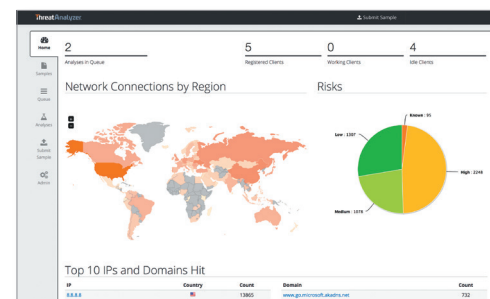
Deep Analysis Creates Actionable Threat Intelligence

Multiple analysis comparison: Quickly spot vulnerabilities with side-by-side comparisons of sample behavior analyzed across various operating systems, patch levels, systems configurations and application versions.

Integrated threat intelligence: Malware behavior reports comprise top-level domains and subdomains flagged during automated analysis, correlating inbound and outbound traffic to potentially malicious IPs supplied by ThreatTrack's ThreatIQ cloud-based threat intelligence services.

Detailed reports: Understand the attributes of the malware samples you analyze so you can deploy resources and cyber defenses to block and eliminate threats, as well as share realtime threat intelligence about your network with team members and executive leadership.

"ThreatAnalyzer can be customized to mirror unique system configurations...for the discovery and elimination of targeted attacks..."
 – IDC Corporation



ThreatAnalyzer provides a dashboard summary view of threat indicators across your sandbox analysis architecture.



PDF Report – Provides an executive summary of an analysis for a sample ideal for sharing or attaching to case files



ZIP Archive – Contains all information captured from analyzed samples, including files created, screenshots, process memory dump and PCAP (network activity)



HTML/XML/JSON Report – Includes complete sample behavioral results, including process details, registry keys, file system modifications, network traffic, URLs, file hashes and more



PCAP File – All network activity generated by a sample during analysis

To learn more about ThreatAnalyzer, send email to Sales@ThreatTrack.com, call +1-855-885-5566 or visit www.ThreatTrack.com/ThreatAnalyzer

© 2015 ThreatTrack, Inc. – ThreatTrack and the ThreatTrack logo are trademarks of ThreatTrack, Inc. in Germany, USA, the United Kingdom and other countries. All product and company names herein may be trademarks of their respective owners. Features are subject to change without notice.

