ANOMALI® ◆◆VMRAY

X-RAY VISION FOR MALWARE

Seamless, integrated Threat Analysis and Intelligence with
VMRay Analyzer and ThreatStream

ANOMALI AND VMRAY JOINT SOLUTION FEATURES:

- Evasion resistant analysis. The VMRay analysis engine runs solely in the hypervisor layer, making it completely invisible to malicious files and URLs, while monitoring every interaction between the malware and the system.

- Full visibility into malware behavior. VMRay technology is unique in that it transparently monitors and logs every interaction between the malware and the operating system.

- Intelligent Monitoring™ for precise, noise-free analysis. Based on years of academic research by VMRay's founders, ITM works much like the zoom lens on a camera, providing only precise, relevant and actionable threat intelligence to security personnel.

- Seamless integration for automatic distribution of IOCs which allows users to immediately operationalize the resulting threat intelligence.

IMMEDIATE TIME-TO-VALUE

- With VMRay Analyzer integrated with ThreatStream, security teams can triage a deluge of samples from multiple sources. VMRay's Now, Near, Deep architecture tightly integrates our groundbreaking dynamic analysis engine with rapid reputation lookup and industry-best static analysis, pre-filtering files for enhanced performance.

- VMRay's powerful analysis engine identifies even the most deeply buried, previously undiscovered malware. A well-designed malware attack can persist and cause harm for months if undetected. VMRay Analyzer sorts the good from the bad and reduces attacker dwell time.

- Innovations such as Intelligent Monitoring™ and smart memory dumping ensure noise-free output and false-positive rates that are near zero: features that enhance team efficiency.

UNPARALLELED MALWARE ANALYSIS AND THREAT DETECTION

VMRay's unique automated malware analysis solution offers unparalleled evasion resistance, noise-free reporting and scalability to handle ever-increasing threat volumes. As a result, organizations can protect critical assets, business processes, and their brand reputation more effectively. Our automated detection scales flexibly to support business growth, ensuring skilled resources and infrastructure are used efficiently and effectively. Security teams can quickly yet comprehensively analyze and detect advanced, zero day and targeted malware.

CRITICAL INTELLIGENCE

The only automated malware analyzer on the market that is truly evasion resistant.

FLEXIBLE DEPLOYMENTS

VMRay offers both cloud and on-premises deployments.

IMMEDIATE RESULTS

Generates a wealth of actionable information that is noise-free with near-zero false-positives.

CASE STUDY

CHALLENGE:

Reduce attacker dwell time.

SOLUTION:

The less time malware is allowed to exist in a system, the better. Analysts use ThreatStream combined with VMRay's comprehensive results to clearly distinguish between artifacts and actionable IOCs. This critical information allows security teams doing threat hunting and incident response to effectively close the door on malware.

VMRay's intuitive and powerful VTI scoring system accelerates the response cycle by providing clear answers to analysts. This full analysis allows cybersecurity teams to reduce attacker dwell time and take prompt remediation steps to prevent future attacks. VMRay's noise-free output can reveal evidence of wider threats including ones that may have been lying dormant for weeks or months.

CUSTOMER BENEFIT:

VMRay Analyzer's full visibility into malware behavior coupled with the ability to distinguish IOCs from artifacts allows cybersecurity teams with ThreatStream to conduct thorough threat hunting operations that leave no stone unturned. Armed with these powerful tools, analysts can uncover things other solutions miss and automate with confidence.

CASE STUDY

CHALLENGE:

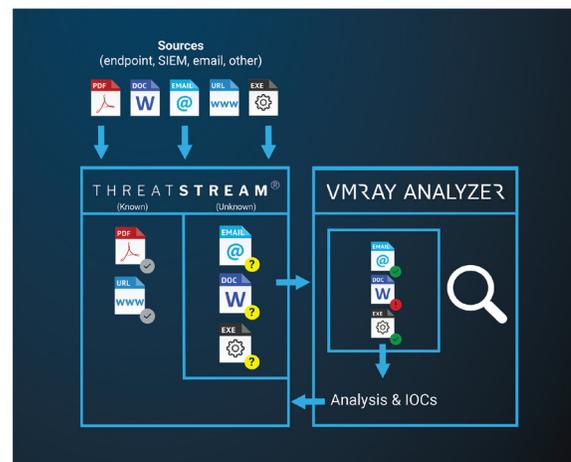Faster incident response through actionable intelligence.

SOLUTION:

Where malware attacks are concerned, a rapid response is essential. VMRay Analyzer is a key tool to quickly and effectively get answers fast for a malware sample within the incident response process.

Using VMRay Analyzer with ThreatStream, cybersecurity teams get total visibility into every interaction between the malware and the operating system with suspicious behavior being clearly flagged without distracting noise. Responders can then take timely corrective action to protect users, applications and IT infrastructure.

CUSTOMER BENEFIT:

Malware can paralyze operations, cut off an organization's revenue and even threaten people's lives. VMRay analysis rapidly points IR specialists toward countermeasures that will disrupt the behavior of the triaged malware, while allowing the healthy parts of the network to operate safely. VMRay Analyzer ensures a more rapid incident response process that leads to the successful containment of malware attacks.

ANOMALI®