RSA ECAT: Signature-less Malware Detection
Detect and investigate advanced threats on endpoints

AT A GLANCE
- Detect previously unknown malware that other solutions miss
- Utilizes a unique signature-less approach
- Delivers actionable intelligence to detect, analyze and respond to advanced threats
- Used in RSA Advanced Cyber Defense services to help organizations in the midst of an attack
- Directly integrates with RSA Security Analytics for complete visibility into endpoint and network activity

CHALLENGES WITH ADVANCED THREATS
Perimeter defenses are inadequate protection against today’s advanced threats. Traditional signature-based approaches leave a gap as attackers continuously use new, hard-to-detect methods to compromise hosts, establish a hidden presence on target systems, and exfiltrate sensitive data out of organizations. Because attackers leverage many established, well exploited antivirus (AV) evasion techniques, the detection rate and effectiveness of traditional, signature-based AV has significantly declined, leaving endpoints vulnerable to zero-day exploits and social engineering of the end user.

Upon detecting anomalous and malicious activity on the network with solutions such as RSA Security Analytics, security analysts must then assess what is happening on the potentially compromised endpoints, where the network traffic is originating or terminating, and capture additional host forensics data for deeper analysis of the attack.

INTRODUCING RSA ECAT- CLOSING THE DETECTION GAP ON ENDPOINTS
Traditional endpoint security products rely on signatures to identify malware, yet this technique has been overwhelmed by the growth of malware and easily bypassed by targeted attacks, such as Advanced Persistent Threats (APTs).

RSA ECAT (Enterprise Compromise Assessment Tool) automates the detection of anomalies on the endpoint. RSA ECAT first creates a baseline of intelligence based on ‘known good’ applications, which filters out the background noise, and then starts detecting and highlighting anomalies from compromised machines. Once a single malicious executable is identified, RSA ECAT can scan across thousands of machines to identify other endpoints that are compromised or at risk.
SIGNATURE-LESS MALWARE DETECTION WITH LIVE MEMORY ANALYSIS

The cornerstone of RSA ECAT’s approach is innovative live memory analysis. The RSA ECAT agent performs per-process live memory analysis and direct physical disk inspection to find traces of compromise and malicious activity. Contrary to the AV or IDS approach of matching suspected malware or traffic patterns with known malware signatures, the ECAT agent gives an x-ray view of what is happening inside a computer’s memory. This accelerates the identification of malware, regardless of whether it has been seen before.

FINDING CODE INJECTION

Instead of creating their own processes and thus risking detection, malware can inject code within trusted applications, such as browsers or Windows services, evading personal firewalls and AV. With RSA ECAT, all running applications are validated by comparing their memory image to the original disk image. This identifies programs modified in memory and locates blocks of injected code.

FINDING ANOMALIES

Malware can also modify internal operating system structures to hide its activity. RSA ECAT performs numerous checks to identify behavior related to malware. By validating important internal kernel and application structures, RSA ECAT identifies anomalies that are typically generated by malware, such as hooking, kernel object modification, file/process/registry/communication hiding, suspicious network traffic and more.

RSA ECAT AND RSA’S ADVANCED CYBER DEFENSE PRACTICE

RSA’s Advanced Cyber Defense (ACD) practice provides services to help with everything from proactive breach readiness assessments to real-time incident response services to assist organizations in the midst of an attack. The RSA ACD Incident Response team leverages the endpoint visibility of RSA ECAT and the log and network packet-based visibility of RSA Security Analytics to gain a holistic view of the infrastructure to quickly uncover and contain even the most advanced threats.

Integration between RSA ECAT and RSA Security Analytics delivers advanced threat detection with the ability to correlate and triage alerts across the network, logs, and endpoints, making security analysts more effective and efficient in their jobs. Security analysts can pivot from in-depth endpoint views to pervasive network and log-based views, thus enabling a seamless cyber investigation that will reduce attacker dwell time in the environment. Together with RSA Security Analytics, RSA ECAT is an integral part of the RSA ACD services and enables security analysts to quickly detect, analyze and respond to even the most advanced threats.

KEY BENEFITS

- Reduce attacker dwell time and the risk of sensitive data exfiltration
- Reduce the time to detect and validate compromised machines
- Reduce incident investigation time with instant actionable intelligence
- Increase visibility of endpoint activity across the enterprise to quickly gauge the magnitude of an intrusion

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.

www.EMC.com/rsa