RSA® Security Analytics

MALWARE ANALYSIS

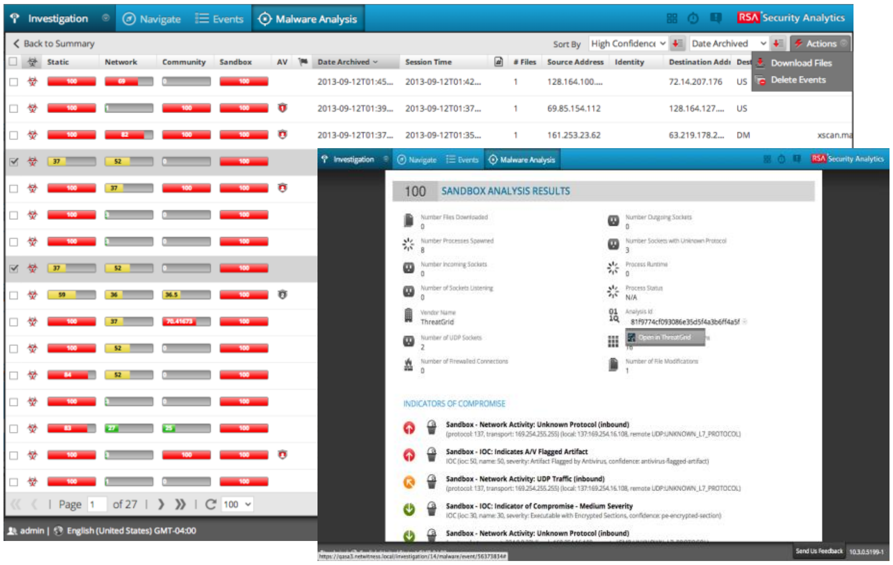
HIGHLIGHTS

Malware Analysis

- Expedites much of an analyst's initial work on an investigation and helps prioritize those files that could be malicious
- Integrated within Security Analytics that helps streamline security operations, reduce costs, and automate manual processes
- Four independent analytical techniques that provide an analyst an impartial view on malware
- Helps identify more sophisticated, zero day attacks and allows you to see the before, during, and after an event

SOPHISTICATED MALWARE TACTICS REQUIRE A UNIQUE APPROACH

Zero-day and targeted malware is successfully compromising your network and evading existing signature-based security technologies, including preventative tools. Why? Modern malware is designed to behave like legitimate traffic and communicate undetected. Malware has become more sophisticated, frequent and stealthy. Security organizations today require a tool that not only identifies potential malicious files using various analytical techniques but also puts context around the attack - to see the before, during and after.



Static	Network	Community	Sandbox	AV	Date Archived	Session Time	# Files	Source Address	Identity	Destination Addr	Dest
100	69	0	100		2013-09-12T01:45...	2013-09-12T01:42...	1	128.164.100....		72.14.207.176	US
100	1	100	100		2013-09-12T01:39...	2013-09-12T01:37...	1	69.85.154.112		128.164.127....	US
100	82	100	100		2013-09-12T01:37...	2013-09-12T01:35...	1	161.253.23.62		63.219.178.2...	DM

100 SANDBOX ANALYSIS RESULTS

Number Files Downloaded: 0
Number Outgoing Sockets: 0
Number Processes Spawned: 8
Number Sockets with Unknown Protocol: 3
Number Incoming Sockets: 0
Process Runtime: 0
Number of Sockets Listening: 0
Process Status: N/A
Vendor Name: ThreatGrid
Analysis Id: 81f9774cf093086e35d5f4a3b6ff4a5f
Number of UDP Sockets: 2
Number of Firewalled Connections: 0
Number of File Modifications: 1

INDICATORS OF COMPROMISE

Sandbox - Network Activity: Unknown Protocol (inbound)
(protocol: 137, transport: 169.254.255.255) (local: 137:169.254.16.108, remote UDP:UNKNOWN_L7_PROTOCOL)

Sandbox - IOC: Indicates A/V Flagged Artifact
IOC (ioc: 50, name: 50, severity: Artifact Flagged by Antivirus, confidence: antivirus-flagged-artifact)

Sandbox - Network Activity: UDP Traffic (inbound)
(protocol: 137, transport: 169.254.255.255) (local: 137:169.254.16.108, remote UDP:UNKNOWN_L7_PROTOCOL)

Sandbox - IOC: Indicator of Compromise - Medium Severity
IOC (ioc: 30, name: 30, severity: Executable with Encrypted Sections, confidence: pe-encrypted-section)

Sandbox - Network Activity: Unknown Protocol (inbound)

AN INTEGRATED, IMPARTIAL APPROACH TO MALWARE

RSA Security Analytics-Malware Analysis is an integrated malware analytical workbench within the Security Analytics platform. As an Investigation application, Malware Analysis allows for the extraction and analysis of suspicious file objects from the traffic stream being captured and expedites much of an analyst's initial work on an investigation and helps prioritize those executables that could be malicious. Advanced security analysts understand that no tool can block all attacks. Malware Analysis helps enable security operations centers identify and mitigate serious problems missed by both traditional and modern approaches to malware protection.

HOW DOES MALWARE ANALYSIS WORK?

RSA Security Analytics Malware Analysis is an analytical toolset and uses a series of analysis techniques, which help automate the workflow of a malware analyst, to gauge the maliciousness of a file sample. The analysis of these sessions results in scores, indicating the probability that the sample is malicious. This probability is exposed through analysis and scoring against the following four methodologies:

NETWORK Examines attributes surrounding the network session for indicators of malicious behavior	• Recursive and Referring Session Analysis • Examples: Country of Origin, Time of Day, Size of Content, Referring Site, TLD and Country Match, JavaScript / Obfuscation, PDF Executable, Alerts present, Streaming Analysis of the Content, intelligence indicators, etc.
STATIC Analyzed for signs of obfuscation	• Scans raw artifacts to predict behavior • Scans for signs of sandbox evasion • Scans DLL import table to predict behavior • Scans raw shell code for well-known malicious shell patterns
COMMUNITY Community-based review by intelligence and reputation partners	• Domain reputation validation via intelligence partners • Known good and bad file validation • Results from more than 40 virus checking providers
ThreatGRID Malware Analysis & Threat Intelligence **(DYNAMIC) SANDBOX** Remote and local dynamic analysis provided by ThreatGRID	• Dynamic file behavior analysis • Tracks submission's network activity, file activity and memory • Fast, real-time, and effective against unknown threats • Provides global context of malicious activity

When combining Malware Analysis' distinct analytic and scoring methods with the unique benefits obtained from the deep visibility into content and behavior, Malware Analysis provides security operation teams an unmatched analytical toolset that revolutionizes the identification, and analysis, and prioritization of malware-based threats to enterprise networks.

APPLIANCE MODEL

SKU	SA-S4H-MAL
Processor	Dual Eight Core, 2.6GHZ
RAM	96GB
Power	750W Redundant
Form Factor	1U, Full Depth
Maximum Weight	44 lbs

The RSA Security Analytics platform includes a limited version of Malware Analysis and Dynamic analysis that is hosted on the Security Analytics web server.

If enterprise requirements exceed the limited version, the Malware Analysis appliance is available.

* Subscriptions to Dynamic analysis provided by ThreatGRID are an additional SKU.