NSE7_ATP-2.5$^{Q\&As}$

Fortinet NSE 7 - Advanced Threat Protection 2.5

QUESTION 1

What information does a scan job report include? (Choose two.)

A. Updates to the antivirus database

B. Summary of the file activity

C. Details about system files deleted of modified

D. Changes to the FortiSandbox configuration

Correct Answer: BC

QUESTION 2

Which FortiWeb feature supports file submission to FortiSandbox?

A. Attack signature

B. Credential stuffing defense

C. IP reputation

D. File security

Correct Answer: C

QUESTION 3

Which threats can FortiSandbox inspect when it is deployed in sniffer mode? (Choose three.)

A. Spam emails

B. Known malware

C. Encrypted files

D. Malicious URLs

E. Botnet connections

Correct Answer: BDE

QUESTION 4

Which of the following actions are performed by FortiSandbox at the static analysis stage?

A. All activity is monitored and recorded while the sample is executed in a virtual environment.

B. The sample\\'s file type is determined and submitted into the appropriate scan job queue.

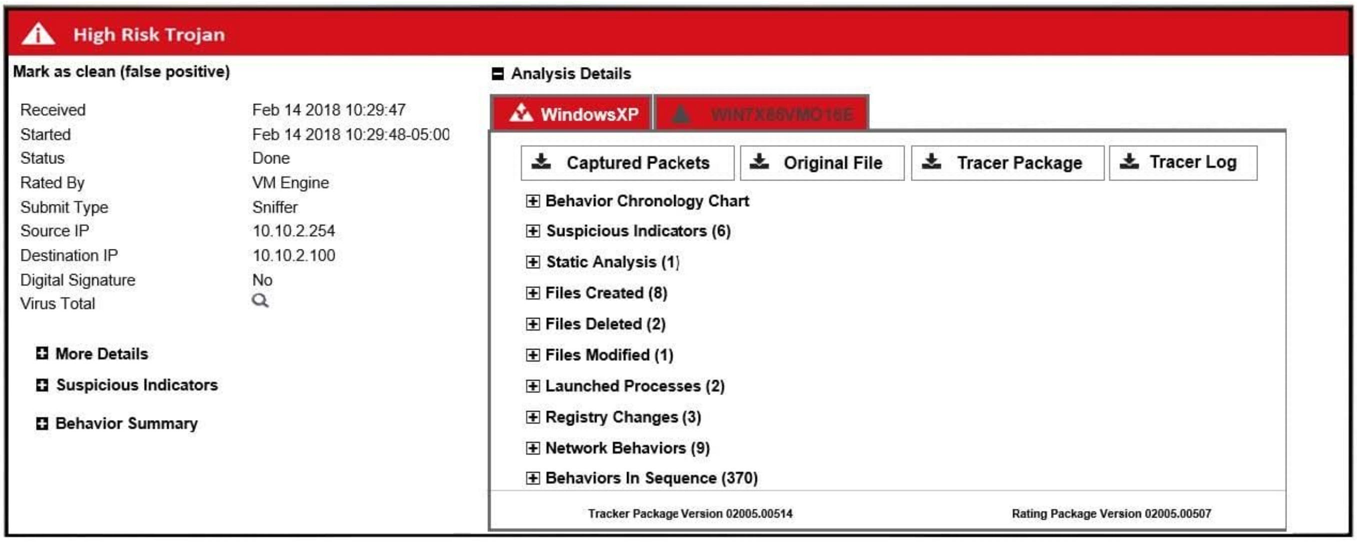
C. The sample behavior is analyzed and embedded objects are extracted for analysis.

D. Embedded attachments are scanned using the FortiGuard antivirus engine and the latest signature database.

Correct Answer: D

QUESTION 5

Examine the scan job report shown in the exhibit, then answer the following question: Which of the following statements are true regarding this verdict? (Choose two.)



Received	Feb 14 2018 10:29:47
Started	Feb 14 2018 10:29:48-05:00
Status	Done
Rated By	VM Engine
Submit Type	Sniffer
Source IP	10.10.2.254
Destination IP	10.10.2.100
Digital Signature	No
Virus Total	

⊞ More Details
⊞ Suspicious Indicators
⊞ Behavior Summary

⊞ Behavior Chronology Chart
⊞ Suspicious Indicators (6)
⊞ Static Analysis (1)
⊞ Files Created (8)
⊞ Files Deleted (2)
⊞ Files Modified (1)
⊞ Launched Processes (2)
⊞ Registry Changes (3)
⊞ Network Behaviors (9)
⊞ Behaviors In Sequence (370)

Tracker Package Version 02005.00514 Rating Package Version 02005.00507

A. The file contained malicious JavaScipt.

B. The file contained a malicious macro.

C. The file was sandboxed in two-guest VMs.

D. The file was extracted using sniffer-mode inspection.

Correct Answer: AC

NSE7_ATP-2.5 PDF Dumps NSE7_ATP-2.5 Practice Test NSE7_ATP-2.5 Braindumps