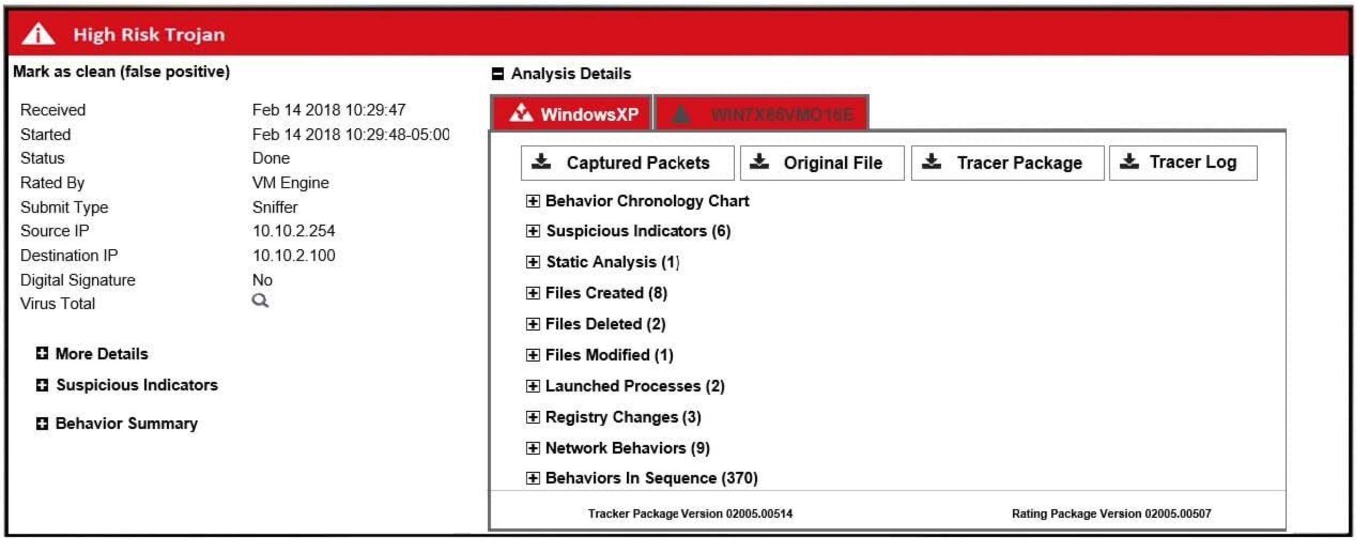
NSE7_ATP-2.5 Q&As

Fortinet NSE 7 - Advanced Threat Protection 2.5

Pass Fortinet NSE7_ATP-2.5 Exam with 100% Guarantee

QUESTION 1

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	

Tracker Package Version 02005.00514 Rating Package Version 02005.00507

A. The file contained malicious JavaScipt.

B. The file contained a malicious macro.

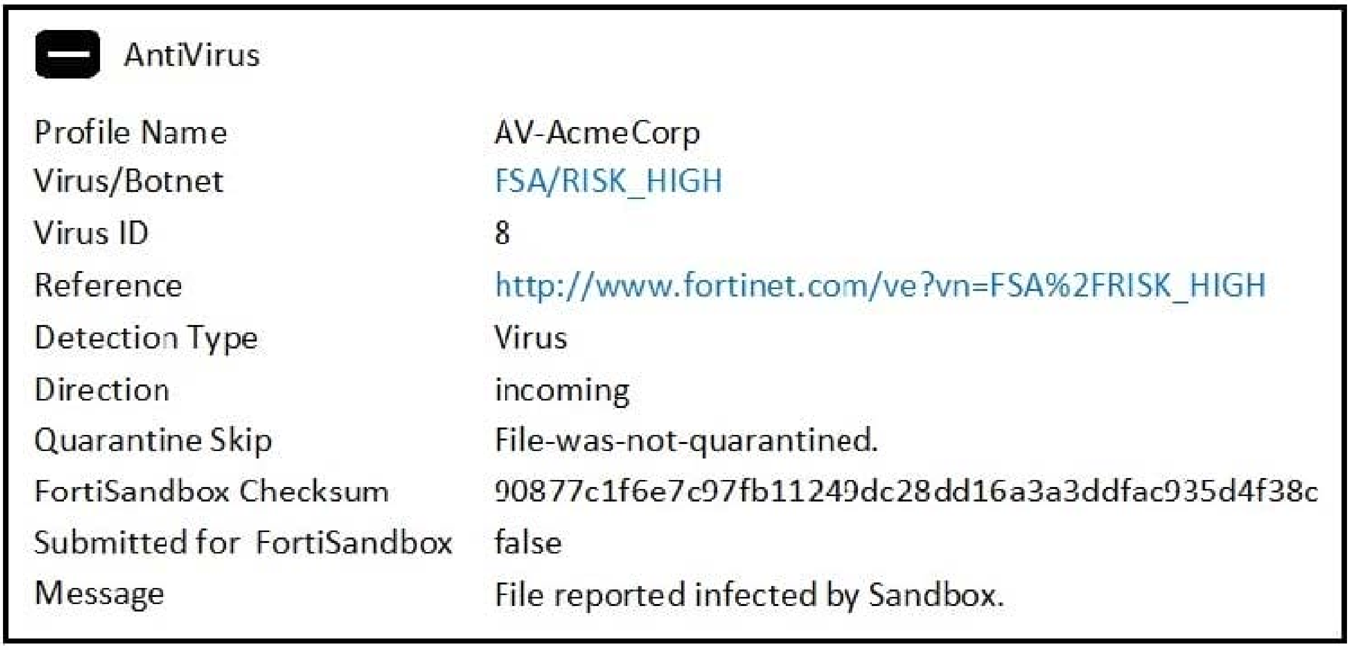
C. The file was sandboxed in two-guest VMs.

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

Correct Answer: AC

QUESTION 2

Examine the FortiGate antivirus log detail shown in the exhibit, then answer the following question:



AntiVirus

Profile Name	AV-AcmeCorp
Virus/Botnet	FSA/RISK_HIGH
Virus ID	8
Reference	http://www.fortinet.com/ve?vn=FSA%2FRISK_HIGH
Detection Type	Virus
Direction	incoming
Quarantine Skip	File-was-not-quarantined.
FortiSandbox Checksum	90877c1f6e7c97fb11249dc28dd16a3a3ddfac935d4f38c
Submitted for FortiSandbox	false
Message	File reported infected by Sandbox.

Which of the following statements is true?

A. FortiGate quarantined the file as a malware.

B. The file matched a FortiSandbox-generated malware signature.

C. The file was downloaded from www.fortinet.com.

D. The FSA/RISK_HIGH verdict was generated by FortiSandbox.

Correct Answer: C

QUESTION 3

Which of the kill chain stages does Fortinet\\'s advanced threat protection solution block? (Choose three.)

A. Command and control

B. Delivery

C. Reconnaissance

D. Lateral movement

E. Weaponization

Correct Answer: ACD

QUESTION 4

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 5

Which of the following advanced threat protection are capable of preventing patient-zero infections? (Choose two.)

A. FortiWeb and FortiSandbox

B. FortiClient and FortiSandbox

C. FortiMail and FortiSandbox

D. FortiGate and FortiSandbox

Correct Answer: AD

FortiGate Enterprise Firewall Platform provides the industry\\'s highest- performing firewall capabilities, and Fortinet\\'s FortiGuard Security Subscription Services provide the industry\\'s highest level of threat research, intelligence, and analytics. Reference: https://www.fortinet.com/content/dam/fortinet/assets/alliances/2019/sb-fortinet-alliancesziften.pdf