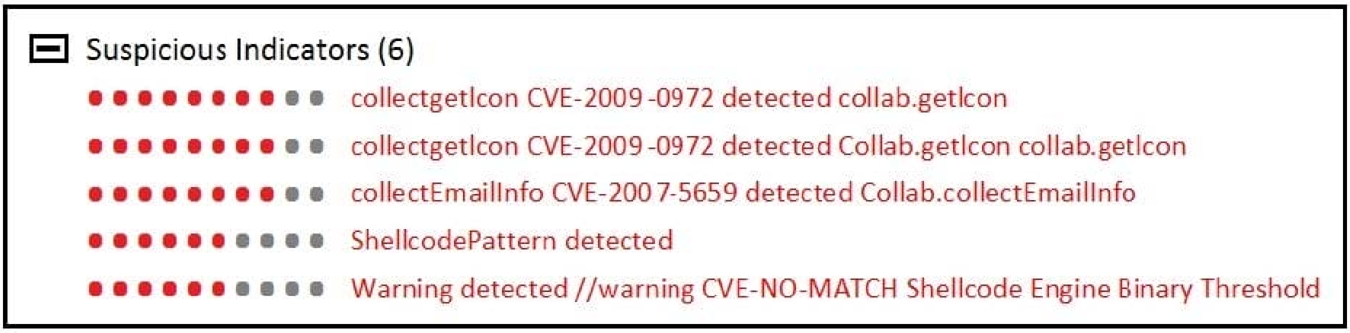
NSE7_ATP-2.5$^{\text{Q\&As}}$

Fortinet NSE 7 - Advanced Threat Protection 2.5

QUESTION 1

Examine the Suspicious Indicators section of the scan job shown in the exhibit, then answer the following question:



Suspicious Indicators (6)

●●●●●●●●●○○ collectgetIcon CVE-2009-0972 detected collab.getIcon

●●●●●●●●●○○ collectgetIcon CVE-2009-0972 detected Collab.getIcon collab.getIcon

●●●●●●●●●○○ collectEmailInfo CVE-2007-5659 detected Collab.collectEmailInfo

●●●●●●○○○○○ ShellcodePattern detected

●●●●●●○○○○○ Warning detected //warning CVE-NO-MATCH Shellcode Engine Binary Threshold

Which FortiSandbox component identified the vulnerability exploits?

A. VM scan

B. Antivirus scan

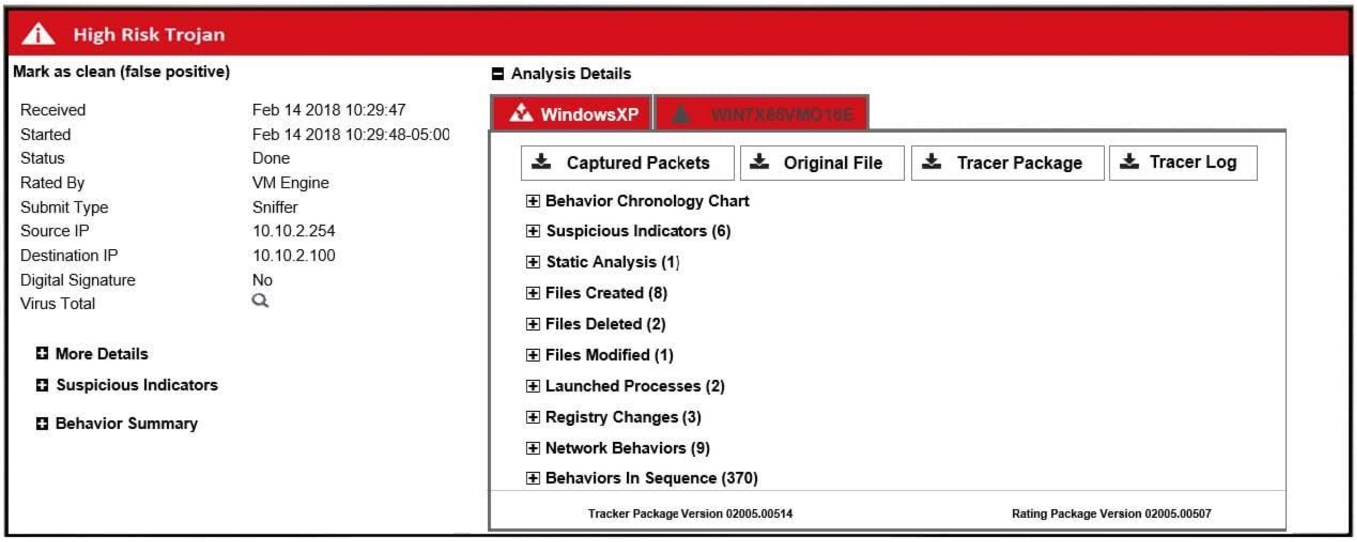
C. Static analysis

D. Cache check

Correct Answer: C

QUESTION 2

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.)



High Risk Trojan

Mark as clean (false positive)

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 3

What advantage does sandboxing provide over traditional virus detection methods?

A. Heuristics detection that can detect new variants of existing viruses.

B. Pattern-based detection that can catch multiple variants of a virus.

C. Full code execution in an isolated and protected environment.

D. Code emulation as packets are handled in real-time.

Correct Answer: A

Heuristic analysis is capable of detecting many previously unknown viruses and new variants of current viruses. However, heuristic analysis operates on the basis of experience (by comparing the suspicious file to the code and functions of known viruses Reference: https://en.wikipedia.org/wiki/Heuristic_analysis

QUESTION 4

Which FortiSandbox interfaces can you use for sniffer mode? (Choose two.)

A. port2

B. port3

C. port1

D. port4

Correct Answer: BC

FortiSandbox reserves port1 for device management and port3 for scanned files to access the Internet.

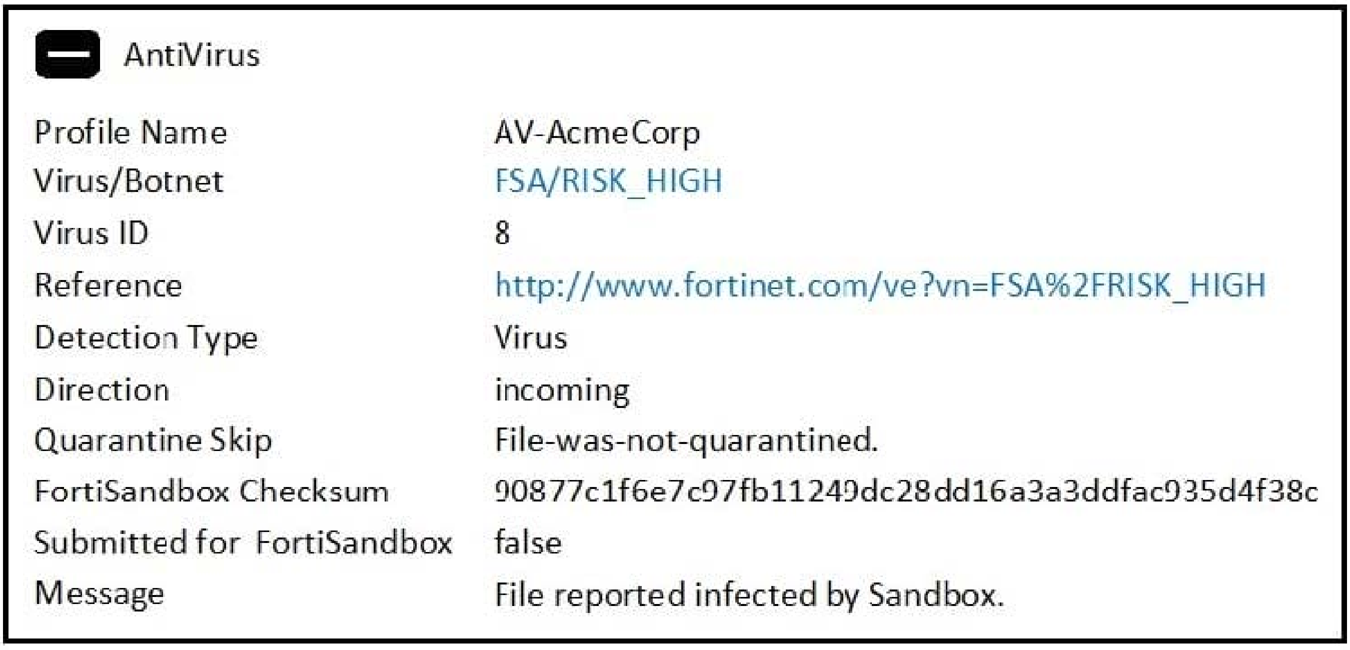
Port1, port3

Reference: https://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%

20Input/500_Sniffer/100_Sniffer.htm

QUESTION 5

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

Latest NSE7_ATP-2.5 Dumps NSE7_ATP-2.5 Study Guide NSE7_ATP-2.5 Braindumps