# NSE7_ATP-2.5.14q

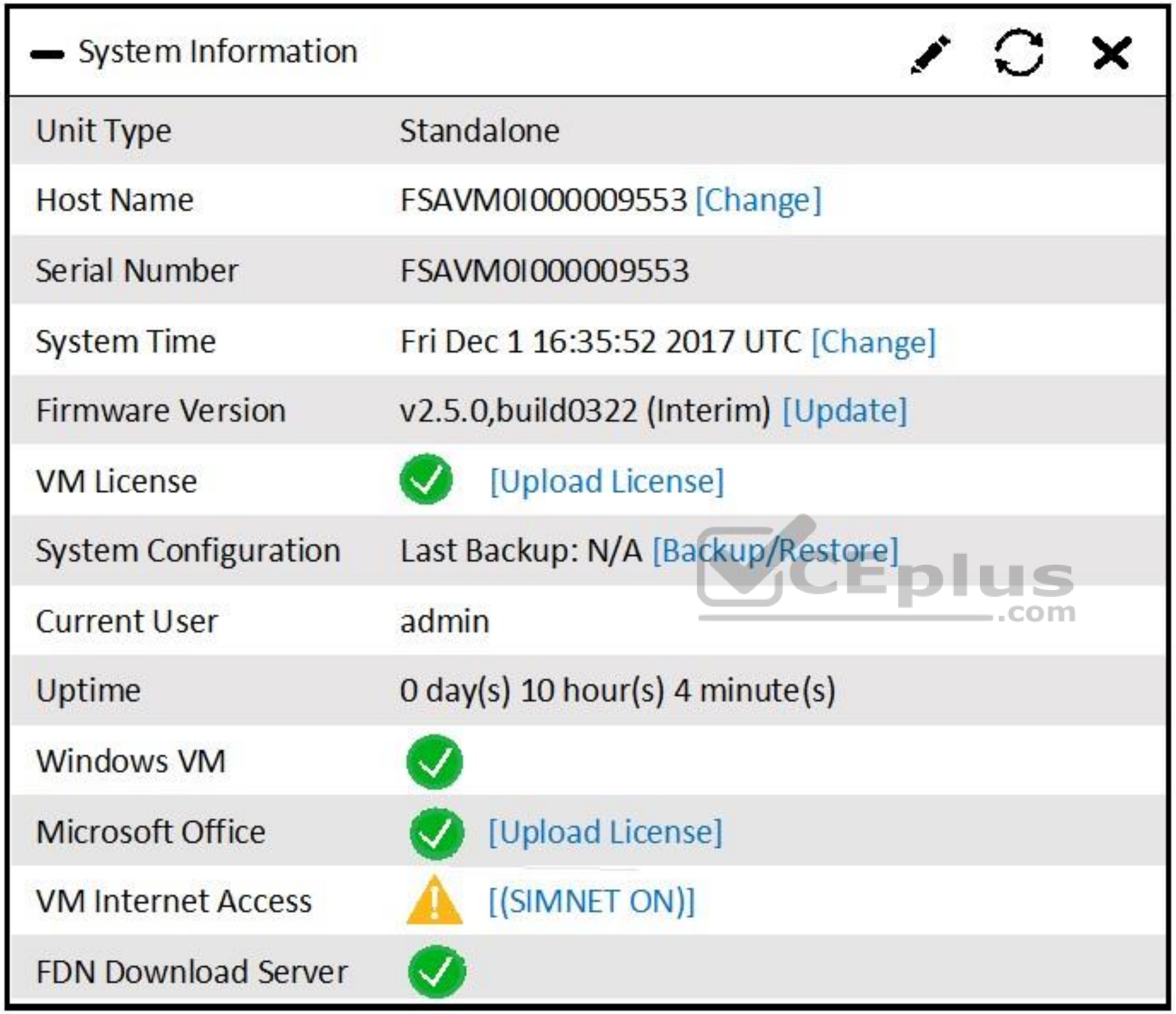
Number: NSE7_ATP-2.5
Passing Score: 800
Time Limit: 120 min

NSE7_ATP-2.5

## Fortinet NSE 7 - Advanced Threat Protection 2.5

## Exam A

**QUESTION 1**
Examine the System Information widget shown in the exhibit, then answer the following question:



System Information

| | |
|---|---|
| Unit Type | Standalone |
| Host Name | FSAVM0I000009553 [Change] |
| Serial Number | FSAVM0I000009553 |
| System Time | Fri Dec 1 16:35:52 2017 UTC [Change] |
| Firmware Version | v2.5.0,build0322 (Interim) [Update] |
| VM License | ✓ [Upload License] |
| System Configuration | Last Backup: N/A [Backup/Restore] |
| Current User | admin |
| Uptime | 0 day(s) 10 hour(s) 4 minute(s) |
| Windows VM | ✓ |
| Microsoft Office | ✓ [Upload License] |
| VM Internet Access | ⚠ [(SIMNET ON)] |
| FDN Download Server | ✓ |

Which of the following inspections will FortiSandbox perform on samples submitted for sandboxing? (Choose two.)

A. URL rating on FQDN seen in DNS requests

B. IP reputation check on callback connections
C. Antivirus inspection on downloaded files
D. URL rating on HTTP GET requests

**Correct Answer:** CD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 2**
Which of the following are features of network share scanning of FortiSandbox? (Choose two.)

A. Move clean files to a separate network share.

B. Replace suspicious files with a replacement message.
C. Detect malicious URLs.D. Detect network attacks.

**Correct Answer:** AB
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Reference: https://help.fortinet.com/fsandbox/olh/2-5-1/Document/900_Scan%20Input/900_Network%20Share/100_Network%20Share.htm

**QUESTION 3**

When using FortiSandbox in sniffer-mode, you should configure FortiSandbox to inspect both inbound and outbound traffic.

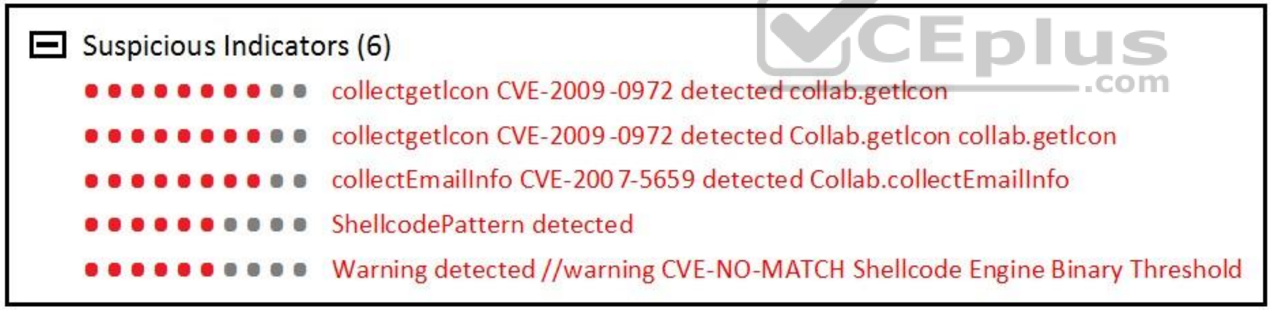
What type of threats can FortiSandbox detect on inbound traffic? (Choose two.)

A. Botnet connections
B. Malware
C. Malicious URLs
D. Intrusion attempts

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
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

**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**

Which advanced threat protection integration solution should you use to protect against out-of-band attack vectors, such as USB drives, used during the delivery stage of the kill chain?

A. FortiGate and FortiSandbox
B. FortiMail and FortiSandbox
C. FortiWeb and FortiSandbox
D. FortiClient and FortiSandbox

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Reference: https://www.infosecpartners.com/fortimail-fortisandbox-perfect-partners/

**QUESTION 6**

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
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:
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-alliances-ziften.pdf

**QUESTION 7**

Which of the following scan job report sections are generated by static analysis? (Choose two.)

A. Office Behaviors

B. Launched Processes

C. Registry Changes D. Virtual Simulator

**Correct Answer:** CD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

Which FortiSandbox diagnostic command should you use to diagnose Internet connectivity issues on **port3**?

A. `ping`

B. `tcpdump`

C. `test-network`

D. `traceroute`

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: https://dokumen.tips/documents/fortios-54-cookbook-fortinet-docs-fortinetknowledgebase-technicaldocumentation-.html

**QUESTION 9**

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

A. Updates to the antivirus database

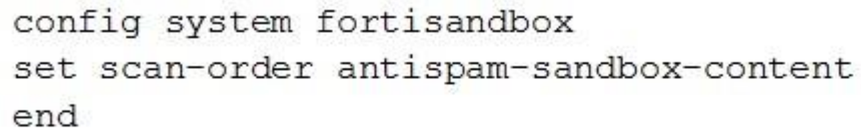
B. Summary of the file activity

C. Details about system files deleted of modified

D. Changes to the FortiSandbox configuration

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
**QUESTION 10**
Examine the CLI configuration, than answer the following question:



```
config system fortisandbox
set scan-order antispam-sandbox-content
end
```

Which of the following statements is true regarding this FortiMail’s inspection behavior?

A. Malicious URLs will be removed by antispam and replaced with a message.
B. Suspicious files not detected by antivirus will be inspected by FortiSandbox.
C. Known malicious URLs will be inspected by FortiSandbox.
D. Files are skipped by content profile will be inspected by FortiSandbox.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 11**
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
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**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 12**

Which FortiWeb feature supports file submission to FortiSandbox?

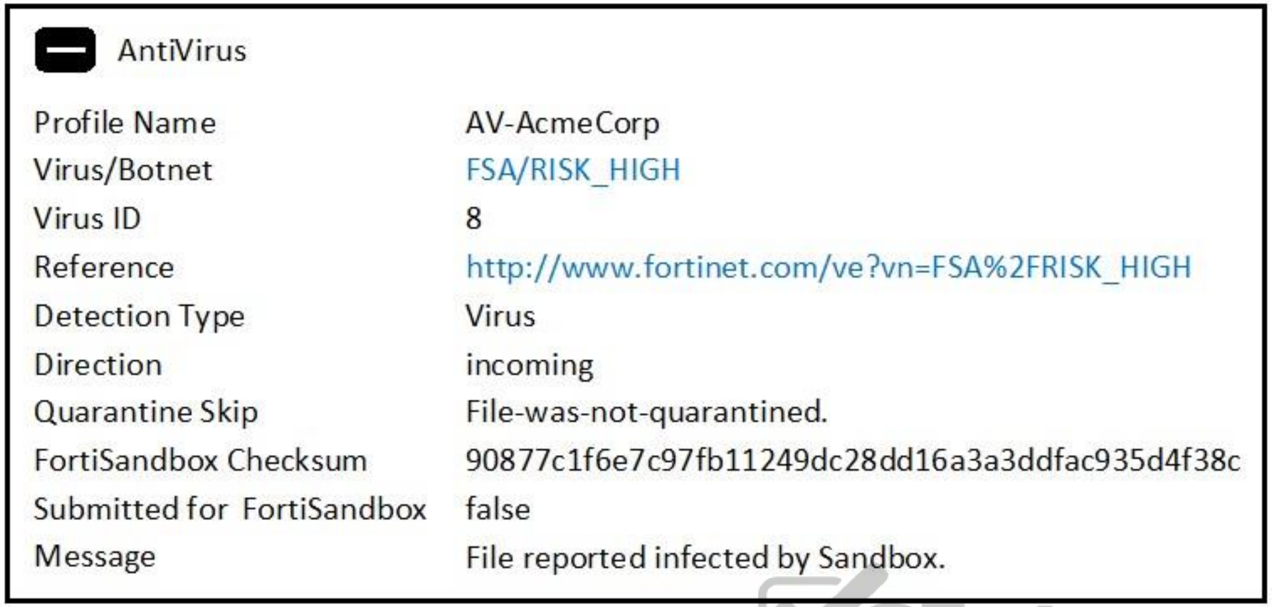
A. Attack signature
B. Credential stuffing defense
C. IP reputation
D. File security

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 13**

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`.

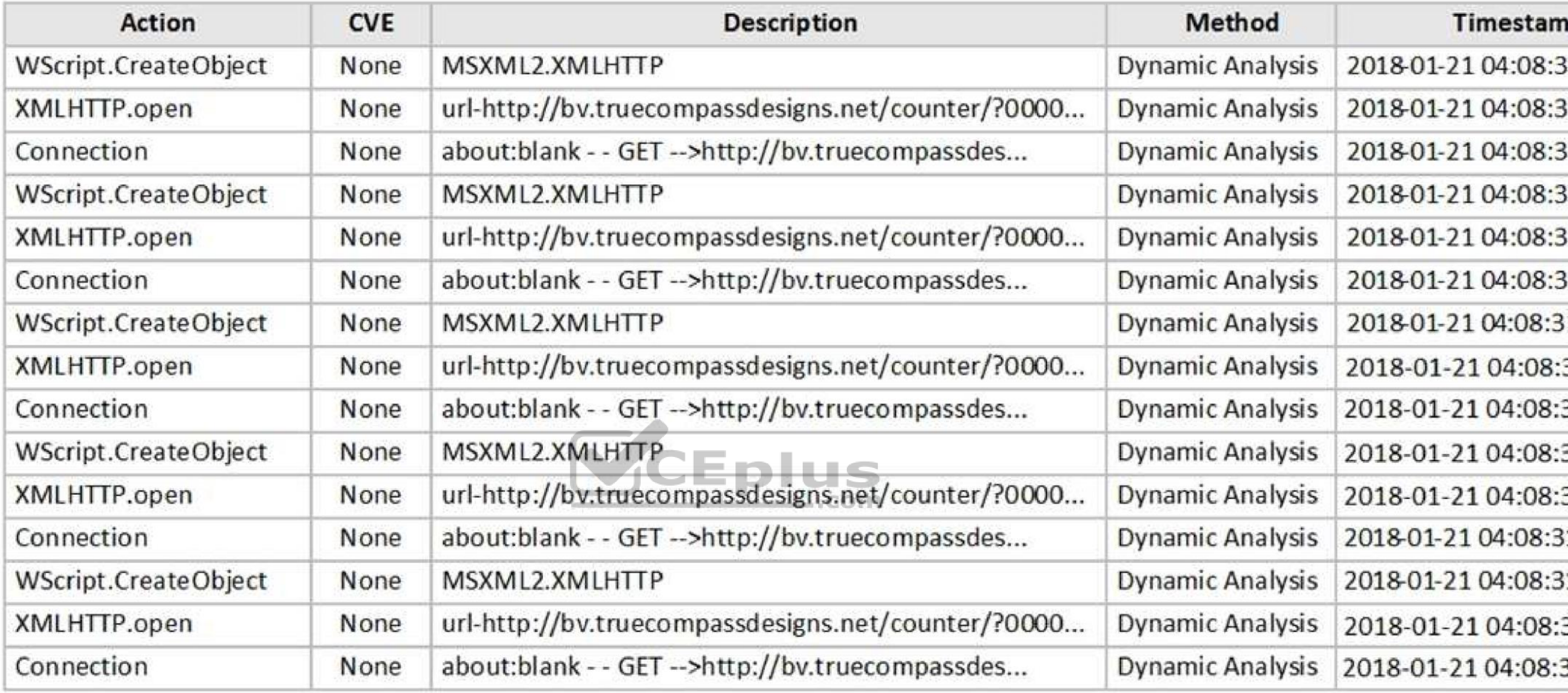
D. The **FSA/RISK_HIGH** verdict was generated by FortiSandbox.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

**QUESTION 14**

Examine the virtual Simulator section of the scan job report shown in the exhibit, then answer the following question:



| Action | CVE | Description | Method | Timestam |
|---|---|---|---|---|
| WScript.CreateObject | None | MSXML2.XMLHTTP | Dynamic Analysis | 2018-01-21 04:08:3 |
| XMLHTTP.open | None | url-http://bv.truecompassdesigns.net/counter/?0000... | Dynamic Analysis | 2018-01-21 04:08:3 |
| Connection | None | about:blank - - GET -->http://bv.truecompassdes... | Dynamic Analysis | 2018-01-21 04:08:3 |
| WScript.CreateObject | None | MSXML2.XMLHTTP | Dynamic Analysis | 2018-01-21 04:08:3 |
| XMLHTTP.open | None | url-http://bv.truecompassdesigns.net/counter/?0000... | Dynamic Analysis | 2018-01-21 04:08:3 |
| Connection | None | about:blank - - GET -->http://bv.truecompassdes... | Dynamic Analysis | 2018-01-21 04:08:3 |
| WScript.CreateObject | None | MSXML2.XMLHTTP | Dynamic Analysis | 2018-01-21 04:08:3 |
| XMLHTTP.open | None | url-http://bv.truecompassdesigns.net/counter/?0000... | Dynamic Analysis | 2018-01-21 04:08:3 |
| Connection | None | about:blank - - GET -->http://bv.truecompassdes... | Dynamic Analysis | 2018-01-21 04:08:3 |
| WScript.CreateObject | None | MSXML2.XMLHTTP | Dynamic Analysis | 2018-01-21 04:08:3 |
| XMLHTTP.open | None | url-http://bv.truecompassdesigns.net/counter/?0000... | Dynamic Analysis | 2018-01-21 04:08:3 |
| Connection | None | about:blank - - GET -->http://bv.truecompassdes... | Dynamic Analysis | 2018-01-21 04:08:3 |
| WScript.CreateObject | None | MSXML2.XMLHTTP | Dynamic Analysis | 2018-01-21 04:08:3 |
| XMLHTTP.open | None | url-http://bv.truecompassdesigns.net/counter/?0000... | Dynamic Analysis | 2018-01-21 04:08:3 |
| Connection | None | about:blank - - GET -->http://bv.truecompassdes... | Dynamic Analysis | 2018-01-21 04:08:3 |

Based on the behavior observed by the virtual simulator, which of the following statements is the most likely scenario?

A. The file contained a malicious image file.
B. The file contained malicious JavaScript.
C. The file contained a malicious macro.
D. The file contained a malicious URL.

**Correct Answer:** B

**Section: (none)**

**Explanation**

**Explanation/Reference:**