

## 300-215<sup>Q&As</sup>

Conducting Forensic Analysis and Incident Response Using Cisco Technologies for CyberOps (CBRFIR)

### Pass Cisco 300-215 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/300-215.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



## QUESTION 1

```
indicator:Observable id= "example:Observable-Pattern-5f1dedd3-ece3-4007-94cd-7d52784c1474">
<cybox:Object id= "example:Object-3a7aa9db-d082-447c-a422-293b78e24238">
<cybox:Properties xsi:type= "EmailMessageObj:EmailMessageObjectType">
<EmailMessageObj:Header>
<EmailMessageObj:From category= "e-mail">
<AddressObj:Address_Value condition= "Contains">@state.gov</AddressObj:Address Value>
</EmailMessageObj:From>
</EmailMessageObj:Header>
</cybox:Properties>
<cybox:Related_Objects>
<cybox:Related_Object>
<cybox:Properties xsi:type= "FileObj:FileObjectType">
<FileObj:File_Extension>pdf</FileObj:File_Extension>
<FileObj:Size_In_Bytes>87022</FileObj:Size_In_Bytes>
<FileObj:Hashes>
<cyboxCommon:Hash>
<cyboxCommon:Type xsi type= "cyboxVocabs:HashNameVocab- 1.0">MD5</cyboxCommon:Type>
<cyboxCommn:Simple_Hash_Value>cf2b3ad32a8a4cfb05e9dfc45875bd70</cyboxCommon:Simple_Ha
sh_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
<cybox:Relationship xsi:type= "cyboxVocabs:ObjectRelatiobshipVocab-
1.0">Contains</cybox:Relationship>
</cybox:Related_Object>|
</cybox:Related_Objects>
</cybox:Object>
</indicator:Observable>
```

Refer to the exhibit. Which two actions should be taken as a result of this information? (Choose two.)

- A. Update the AV to block any file with hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".
- B. Block all emails sent from an @state.gov address.
- C. Block all emails with pdf attachments.
- D. Block emails sent from Admin@state.net with an attached pdf file with md5 hash "cf2b3ad32a8a4cfb05e9dfc45875bd70".
- E. Block all emails with subject containing "cf2b3ad32a8a4cfb05e9dfc45875bd70".

Correct Answer: AB

## QUESTION 2

A security team received reports of users receiving emails linked to external or unknown URLs that are non-returnable and non-deliverable. The ISP also reported a 500% increase in the amount of ingress and egress email traffic received. After detecting the problem, the security team moves to the recovery phase in their incident response plan. Which two actions should be taken in the recovery phase of this incident? (Choose two.)

- A. verify the breadth of the attack
- B. collect logs
- C. request packet capture
- D. remove vulnerabilities
- E. scan hosts with updated signatures

Correct Answer: DE

---

### QUESTION 3

```
GET /wp-content/rm1q_q6x4_15/ HTTP/1.1
Host: iraniansk.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 10 Aug 2020 20:16:17 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 10 Aug 2020 20:16:17 GMT
Content-Disposition: attachment; filename="Fy.exe"
Content-Transfer-Encoding: binary
Set-Cookie: 5f31ab113af08=1597090577; expires=Mon, 10-Aug-2020 20:17:17 GMT; Max-Age=60; path=/
Last-Modified: Mon, 10 Aug 2020 20:16:17 GMT
Vary: Accept-Encoding, User-Agent

6000
MZ.....@.....I.L!This program cannot be run in DOS mode

$ N3 'JM' J' 'l'0' - 'Rich
PE L fl_ t J @
f
0 @ < L @ text s t
rdata x @ @data _ 0 $ @ rsrc
8 @
@
8
Vj 6 B ^ A J
Q R $ I Y V DS tV Y ^ V Nt ^ B j r8 % j x e x F
I M x
3 Vj jd AB B ^ A 'B B V B DS tV 0 Y ^ U u u u u C E | U u u u u E
] $ u $ U u u 4 B u l V P 8 8 t ( u u @ B M v ; s l t V u ; r 3
# ^ ] DS @ j P t $ 0 B u t $ T $ z 0 d 0 $ SY DS T $ k @ Ts u DS DS T s k |
@@ T $ u DS VW @ x 5 0 C v 0 U YP Y ; D $ t 6 ; u 3 _ ^ F U Sp < C 3 e S w
3
A D
] 3 t u y N Fu S @ = | e ~ y + M U @ y H
@ U y J B U y l A
U 2 : G M u ^ 3 ] U SC e e u 3 = SC t M V M M 0 j M Q @ V E
E ] E P E u V SC | E t M E ^ A x D S V I D ( t H + ^ I D ( t M +
$ Vt-qA r 9 T $ t r l L S v 2 ^ U M w 3 Q | Y
3 s e E P M h B E P E B < V t s k B ^ t $ t $ t $ q L 8 t $ q 8 j q 8 j q
8 D $ t $ P F c L $ @ O P B D $ | B B h w 3 P P t $ t $ t $ P j B

1 client pkt, 231 server pkts, 1 turn

Entire conversation (290kB) Show and save data as ASCII Stream 2
```

Refer to the exhibit. According to the Wireshark output, what are two indicators of compromise for detecting an Emotet malware download? (Choose two.)

- A. Domain name:iraniansk.com
- B. Server: nginx

C. Hash value: 5f31ab113af08=1597090577

D. filename= "Fy.exe"

E. Content-Type: application/octet-stream

Correct Answer: CE

#### QUESTION 4

```
<stix:Indicator id= "CISA:Indicator-18559cbf-57ce-49ba-bb73-2bdf5426744c" timestamp= "2020-04-08T00:44:39.970278+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-dd7a25ea-830f-46cd-9d2a-d7b5aa354f89">
<cybox:Object id= "CISA:Object-a2169ad2-5273-41cb-9491-48c69b22da74">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals" >Fightcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-2035a032-6b8d-4dd9-8752-7316af76e702" timestamp= "2020-04-08T00:44:39.970417+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-463472d3-e45e-46c1-bf05-da7458cb943c">
<cybox:Object id= "CISA:Object-7728bd69-e724-4917-9550-9ae853becf28">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">nocovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
<stix:Indicator id= "CISA:Indicator-8b56999b-a015-4399-ab80-cca9bcaf7ebf" timestamp= "2020-04-08T00:44:39.970554+00:00" xsi:type= "indicator:IndicatorType">
<indicator:Title>Malicious FQDN Indicator</indicator:Title>
<indicator:Observable id= "CISA:Observable-0648e1db-aa4e-4aca-914e-ea0ccd445254">
<cybox:Object id= "CISA:Object-db21b6ca-0c1b-474d-8bf7-950ead2d9760">
<cybox:Properties xsi:type= "DomainNameObj:DomainNameObjectType" type= "FQDN">
<DomainNameObj:Value condition= "Equals">stopcovid19.shop</DomainNameObj:Value>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
```

Refer to the exhibit. Which two actions should be taken based on the intelligence information? (Choose two.)

A. Block network access to all .shop domains

B. Add a SIEM rule to alert on connections to identified domains.

- C. Use the DNS server to block hole all .shop requests.
- D. Block network access to identified domains.
- E. Route traffic from identified domains to block hole.

Correct Answer: BD

---

## QUESTION 5

An engineer is analyzing a ticket for an unexpected server shutdown and discovers that the web-server ran out of useable memory and crashed.

Which data is needed for further investigation?

- A. /var/log/access.log
- B. /var/log/messages.log
- C. /var/log/httpd/messages.log
- D. /var/log/httpd/access.log

Correct Answer: B

---

## QUESTION 6

An engineer received a report of a suspicious email from an employee. The employee had already opened the attachment, which was an empty Word document. The engineer cannot identify any clear signs of compromise but while reviewing running processes, observes that PowerShell.exe was spawned by cmd.exe with a grandparent winword.exe process. What is the recommended action the engineer should take?

- A. Upload the file signature to threat intelligence tools to determine if the file is malicious.
- B. Monitor processes as this a standard behavior of Word macro embedded documents.
- C. Contain the threat for further analysis as this is an indication of suspicious activity.
- D. Investigate the sender of the email and communicate with the employee to determine the motives.

Correct Answer: A

---

## QUESTION 7

**Alert Message**

SERVER-WEBAPP LOCK WebDAV Stack Buffer Overflow attempt

**Impact:**

CVSS base score 7.5

CVSS impact score 6.4

CVSS exploitability score 10.0

Confidentiality Impact PARTIAL

integrity Impact PARTIAL

availability Impact PARTIAL

Refer to the exhibit. After a cyber attack, an engineer is analyzing an alert that was missed on the intrusion detection system. The attack exploited a vulnerability in a business critical, web-based application and violated its availability. Which two migration techniques should the engineer recommend? (Choose two.)

- A. encapsulation
- B. NOP sled technique
- C. address space randomization
- D. heap-based security
- E. data execution prevention

Correct Answer: CE

---

**QUESTION 8**

An engineer is investigating a ticket from the accounting department in which a user discovered an unexpected application on their workstation. Several alerts are seen from the intrusion detection system of unknown outgoing internet traffic from this workstation. The engineer also notices a degraded processing capability, which complicates the analysis process. Which two actions should the engineer take? (Choose two.)

- A. Restore to a system recovery point.
- B. Replace the faulty CPU.
- C. Disconnect from the network.

- D. Format the workstation drives.
- E. Take an image of the workstation.

Correct Answer: AE

---

#### QUESTION 9

An "unknown error code" is appearing on an ESXi host during authentication. An engineer checks the authentication logs but is unable to identify the issue. Analysis of the vCenter agent logs shows no connectivity errors. What is the next log file the engineer should check to continue troubleshooting this error?

- A. /var/log/syslog.log
- B. /var/log/vmksummary.log
- C. var/log/shell.log
- D. var/log/general/log

Correct Answer: A

Reference: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.monitoring.doc/GUID-832A2618-6B11-4A28-9672-93296DA931D0.html>

---

#### QUESTION 10

00386078	64	44	45	33	4C	6A	41	34	4C	6A	4D	78	4C	6B	5A	44
00386088	4D	41	59	78	4E	79	34	31	4E	54	41	32	4C	6A	55	31
00386098	4D	44	59	75	4E	6A	67	7A	4E	77	3D	3D	00	AB	AB	AB

Refer to the exhibit. Which encoding technique is represented by this HEX string?

- A. Unicode
- B. Binary
- C. Base64
- D. Charcode

Correct Answer: B

Reference: <https://www.suse.com/c/making-sense-hexdump/>