300-215 Q&As

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.geekcert.com/300-215.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1


```
<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 2

```
"pattern": "[url:value = 'http://x4z9rb.cn/4712/']",
        "pattern_type": "stix",
        "valid_from": "2014-06-29T13:49:37.079Z"
 },
 {
        "type": "malware",
        "spec_version": "2.1",
        "id": "malware--162d917e-766f-4611-b5d6-652791454fca",
        "created": "2014-06-30T09:15:17.182Z",
        "modified": "2014-06-30T09:15:17.182Z",
        "name": "x4z9arb backdoor",
```

Refer to the exhibit. What is the IOC threat and URL in this STIX JSON snippet?

A. malware; `http://x4z9arb.cn/4712/\\'

B. malware; x4z9arb backdoor

C. x4z9arb backdoor; http://x4z9arb.cn/4712/

D. malware; malware--162d917e-766f-4611-b5d6-652791454fca

E. stix; `http://x4z9arb.cn/4712/\\'

Correct Answer: D

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

$.....N3..'..'..'JM'..'J['..'.I'0.'...'..'...'–.'...'.'...'.'...'..'Rich.
'.....PE..L...f1_.....t..J.....@.....
.....f.....
0....@.....<.....L....@.....text.....s.....t.....
..'.rdata.....x.....@..@.data.....__.0..$.....@....rsrc.....
8.....@..
@.....
.....8..
.Vj.....6.....B...^..A.....J...
.....Q..R...t$..I...Y.....V.....DS..t.V.....Y.^.....V..Nt.....^.B.jj.r8.%....j...x.....e.....x.....F
...I.....M...x.....
3.....Vj.jd...AB.....B..^..A...'B.....B.....V.....B.....DS..t.V.0..Y.^.U.u.u.u.u.C..E.....|.U...u.u.u.u.....E
...].|$...u.....t$.....U...u.u..4.B...u.IVP.8.8....t(.u.u..@.B.M....v;.s.I....tV.u;.r.3..
.....#,^].DS.....@..j.P.t$..0.B...u..t$.T.t$..z.....0d.0.....$.SY.DS...T$.k.@..Ts.....u.DS..DS..Ts.k.I
@@...T$.....u.D$.VW.....@.x.....5.0C...v0.U.....YP.....YY;D$.t.6;u.3._^.F.U.Sp.....<C.3.....e...SvW.....
3.....,
...A.....D
.|.3..t..u.....y.N.....F.u...S....@=.....|.....e...~y.....+.M.U@....y.H
...@.....U.....y.J.....B.....U.....y.I.....A.
.....U.2..'.G.M.u.....^3[.....U.....SC.e.e...u.3.....=.SC.t.M.V.M.M.0j.M.Q...@.V.E.
....E.....|",E.P.E.P.u.V...SC...|.E.t.M...E.^.Ax.DS.V.....I.D.(,,t,.H...+....^.....I.D.(.t.M...+.....|
$..Vt-q.A....r.....9T$.r....r...I....;LS.v...2.^.....U.M...w.3.Q.|...Y.....
3.....s..e...E.P.M....'...h.B.E.P.E...B...<...V.ts...k.....B...^...t$.t$.t$.q.L.8...t$.q...8...j.q....8.j...q
...8...D$..t$.P.F.....c.....L$.@.OP...B....D$...|.....,B...B.....hw.....3.PP.t$.t$.t$.t$.Pj.....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

An organization recovered from a recent ransomware outbreak that resulted in significant business damage. Leadership requested a report that identifies the problems that triggered the incident and the security team\\'s approach to address these problems to prevent a reoccurrence. Which components of the incident should an engineer analyze first for this report?

A. impact and flow

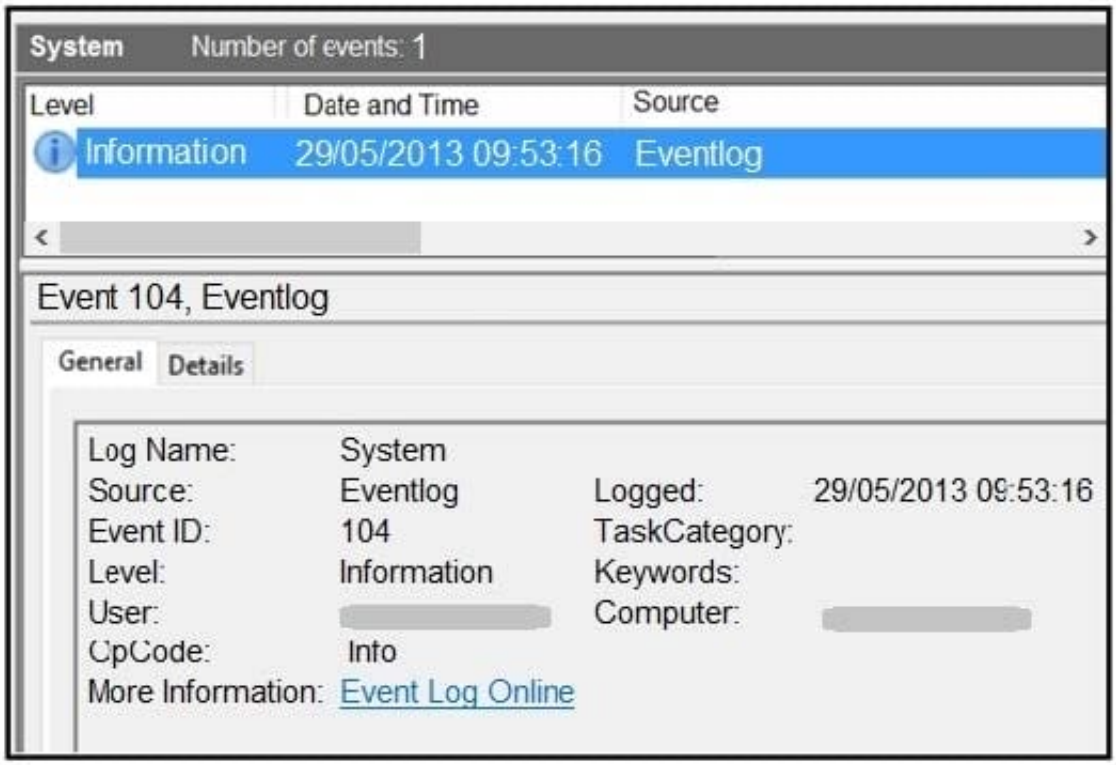
B. cause and effect

C. risk and RPN

D. motive and factors

Correct Answer: D

QUESTION 5



Refer to the exhibit. An employee notices unexpected changes and setting modifications on their workstation and

creates an incident ticket. A support specialist checks processes and services but does not identify anything suspicious. The ticket was escalated to an analyst who reviewed this event log and also discovered that the workstation had multiple large data dumps on network shares. What should be determined from this information?

A. data obfuscation

B. reconnaissance attack

C. brute-force attack

D. log tampering

Correct Answer: B