ANSWERS

F11.2 Malware

Cyber security · GCSE · OCR J277 1.4.1, AQA 8525 3.6.2, Edexcel 1CP2 5.3.1 · about 15 min

BugBotLab

What this lesson is about

Viruses, worms, trojans, ransomware and spyware, and a signature scanner.

- Kinds of malware
- How malware gets in
- Signs of infection
- A signature scanner

Questions

6 marks in all

1. How does a worm spread? [1 mark]

- ☐ **A** By itself across a network
- ☐ **B** Only when a user opens an infected file
- ☐ **C** By pretending to be a useful program
- ☐ **D** It cannot spread

> **Answer:** A. A worm needs no user action; a virus needs a file to be run.

2. What does ransomware do? [1 mark]

- ☐ **A** Encrypts your files and demands payment for the key
- ☐ **B** Shows adverts
- ☐ **C** Records what you type
- ☐ **D** Speeds up your computer

> **Answer:** A. It holds your data hostage.

3. What is a trojan? [1 mark]

- ☐ **A** Malware disguised as something useful so you install it
- ☐ **B** Malware that spreads by itself
- ☐ **C** Software that removes viruses
- ☐ **D** A kind of firewall

> **Answer:** A. It tricks you into installing it, then does harm.

4. What does spyware do? [1 mark]

- ☐ **A** Secretly watches what you do, such as recording keystrokes
- ☐ **B** Encrypts your files
- ☐ **C** Floods a network
- ☐ **D** Blocks adverts

> **Answer:** A. It steals information quietly.

5. Why can a signature scanner miss new malware? [1 mark]

- ☐ **A** It only knows patterns it has seen before
- ☐ **B** It scans too slowly
- ☐ **C** It needs the internet
- ☐ **D** It only scans images

> **Answer:** A. Brand-new malware has no known signature yet.

6. What does this program print? [1 mark]

```
sigs = ["evil", "steal"]
text = "steal_data()"
print([s for s in sigs if s in text])
```

> **Answer:**
>
> ```
> ['steal']
> ```
>
> Only 'steal' appears in the text.

The task: a malware scanner

Complete the scanner. For each file in `files`, find every signature from `signatures` that appears in its contents. Print `<name>: INFECTED (<signatures>)` with the matches joined by `, `, or `<name>: clean`. At the end print `infected files: <n>`.

```
# the two lines every program starts with: the commands, then the robot
from bugbot import *
connect()

signatures = ["keylog", "ransom", "botnet", "backdoor"]
files = {
    "snake.py": "print('score', score)",
    "update.exe": "install backdoor and keylog",
    "photo.jpg": "holiday beach sunset",
    "free_robux.exe": "encrypt files then ransom the user",
}
```

The hint students can ask for: For each file, collect every signature that appears anywhere in its contents. A file with any matches is infected and you list them; a file with none is clean. Count the infected ones as you go.

A solution

```
from bugbot import *
connect()
signatures = ["keylog", "ransom", "botnet", "backdoor"]
files = {
    "snake.py": "print('score', score)",
    "update.exe": "install backdoor and keylog",
    "photo.jpg": "holiday beach sunset",
    "free_robux.exe": "encrypt files then ransom the user",
}
infected = 0
for name, contents in files.items():
    hits = [s for s in signatures if s in contents]
    if hits:
        print(f"{name}: INFECTED ({', '.join(hits)})")
        infected = infected + 1
    else:
        print(f"{name}: clean")
print("infected files:", infected)
```

Any program that meets the task's checks is marked correct in the simulator; this is one way, not the only way.