WORKSHEET

# 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

Name _____ Class _____ Date _____

## 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

**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

**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

**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

**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

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

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

**Plan your program here, then type it in and press Run.**

**Do it on the robot**

www.bugbotlab.com/learn/f11-2-malware/

The simulator checks it and tells you when it passes. Nothing to install, no account.

## Challenges

1. Make the scan ignore capital letters, so `Ransom` is caught too.
2. For each infected file, say which kind of malware its signature suggests.
3. Why can a signature scanner never catch brand-new malware?