AP CYBERSECURITY • EXERCISE SHEET

4.1 Device Vulnerabilities and Attacks

Name: _____ Class: _____ Date: _____ **Total: 9 marks**

KEY WORDS malware 恶意软件 • virus 病毒 • worm 蠕虫 • iot 物联网 • ransomware 勒索软件

Objective

Build the skills to answer exam questions on device types and **malware** 恶意软件.

You must be able to:

- identify types of device, including **IoT** 物联网 devices
- name malware by its behaviour (virus, worm, ransomware, RAT, rootkit)
- rate device risk high, moderate, or low

1 Worked examples

Study these first. Each one shows the method for a task used later.

■ Naming malware

A virus needs a user to run a file. A worm spreads by itself. Ransomware encrypts files for money. A remote access trojan (RAT) gives remote control. A rootkit hides deep in the OS.

■ Rating device risk

High = an unpatched critical device (e.g. a hospital server). Low = a low-value device with an unused open port. The value and criticality of the device set the level.

2 Practice

2.1 State the key difference between a virus and a worm. [2]

2.2 Name the malware that encrypts a victim's files and demands payment. [1]

2.3 An organisation has not applied a critical security update to its email server.

(a) State the risk level. [1]

(b) Justify your answer. [1]

3 Exam-style questions

3.1 Which malware spreads across a network WITHOUT any user action? [1]

- **A** virus
- **B** worm
- **C** trojan
- **D** spyware

3.2 An internet-connected thermostat is an example of a(n) [1]

- **A** server
- **B** IoT device
- **C** mainframe
- **D** firewall

3.3 Malware on a device gives an adversary full remote control of it.

(a) Name the type of malware. [1]

(b) State one action the adversary could then take. [1]

Solutions

2.1 a virus needs a user to open/run a file; a worm spreads by itself with no human action.

2.2 ransomware.

2.3 (a) high. (b) an unpatched critical service can be exploited with serious impact.

3.1 B. a worm self-spreads; a virus needs a user.

3.2 B. everyday embedded connected devices are IoT devices.

3.3 (a) a remote access trojan (RAT). (b) e.g. steal files, watch the user, or use it as a foothold.