MODULE G SECURITY · G1

Malware: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.1 (processes and aim of cyber security threats: malware: virus, worm, Trojan horse, spyware, adware, ransomware)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. A bullet starting "..." builds on the one before it. Credit any other valid answer that shows the same understanding. Anti-malware and other solutions are tested in G7.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.1	One mark for each correct type: Unwanted adverts, redirects searches: adware Standalone, copies itself across a network: worm Encrypts files, demands payment: ransomware Looks genuine, hidden harmful code: Trojan horse Attaches to a file / program: virus Monitors user, sends data to a third party: spyware	**6**	Accept "Trojan" for Trojan horse. Ignore capitals and minor spelling errors if the type is clear. Do not accept "malware" or "hacking" for any row. Accept "keylogger" for the spyware row.
2(a) 0478 5.3.1	Any two from: The worm replicates / copies itself ... and sends / moves the copies across the network to other (connected) computers It does not need to attach to a host file / program // it is standalone It does not need any user action / input (to spread) It uses weaknesses / security holes / vulnerabilities in software / the operating system (to get onto other computers)	**2**	max 2. Do not accept "it is sent by email by the user" (that needs user action).
2(b) 0478 5.3.1	Any two from: Uses up / takes up bandwidth // slows the network down Takes up storage / memory space Slows down / crashes the computers Deletes / damages / corrupts data / files Opens back doors (to the computers) // lets a hacker gain access Installs / delivers other malware (onto networked computers) The network / systems may have to be shut down / taken offline (to remove it)	**2**	max 2. Do not accept "it spreads" alone (that is how, not an effect).

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) 0478 5.3.1	Any three from: The ransomware gets onto the system (e.g. through an email attachment / a link / a download / removable media) It encrypts the data / files (on the firm's computers / system) ... so the firm cannot access / use its data / files / computers A message / demand for payment / a ransom (fee) is displayed ... the decryption key is only given if the fee is paid // the files are only "released" if the fee is paid The attacker may threaten to delete / publish the data (if the fee is not paid) Paying does not guarantee the files will be decrypted	**3**	max 3. Accept "locks" for encrypts. Do not accept "it steals the files" alone.
3(b) 0478 5.3.1	Any one from: To extort money // to get the victim to pay a fee / ransom (to unlock / decrypt the data)	**1**	Accept "to make money from the victim". Do not accept "to encrypt files" (that is the process, not the aim).
4(a) 0478 5.3.1	Any two from: The spyware monitors / records key presses // acts as a keylogger ... it captures the username / password (as it is typed) The data is sent to a third party / the attacker ... who uses the log-in details to log in to the accounts	**2**	max 2. Accept "records screen activity / what the user types" for MP1. Do not accept "it hacks the account" alone.
4(b) 0478 5.3.1	Any two from: Displays / generates unwanted adverts / pop-ups Redirects the browser / searches / user to other / fake / unsafe websites Slows down the computer // reduces internet speed / performance Adverts, when clicked, may link to / download other malware / viruses May contain spyware // may collect data about the user / browsing May change browser settings / the home page // can be hard to remove	**2**	max 2. Two different effects needed.
5(a) 0478 5.3.1	A virus needs a host file / program: True A Trojan horse copies itself on its own: False Some adware contains spyware: True	**3**	One mark per correct row. A row with both boxes ticked scores 0.

Total: 21 marks