CYBERQUIZZER CHEAT SHEET

Malware Types

Classification hangs on two questions: **how does it spread**, and **what does it want**. Get those right and every exam item follows.

Scan to drill this sheet

Virus vs worm vs trojan

The one comparison every exam asks. It comes down to how each one travels.

	Virus Needs a host file	Worm Needs nothing	Trojan Needs you
Spreads by	Attaching to a file that a user then runs or shares	Copying itself across the network on its own	Pretending to be software you wanted to install
Self-replicates	Yes — but only when the host runs	Yes — autonomously, no user at all	No — it does not replicate
User action	Required — someone must open the host	None — exploits a service directly	Required — the user installs it willingly
The tell	Infected files; "attached to", "infects"	"Spread across the network without user interaction"	"Disguised as", "appeared to be legitimate"
Example	Melissa, macro viruses in Office docs	WannaCry, Conficker, Stuxnet	Emotet, fake "codec" and cracked installers

The rest of the family

Classified by payload — what it does once it is in. A sample can be several of these at once.

Ransomware

Encrypts data and demands payment. Modern strains exfiltrate first, then threaten to leak — "double extortion".

Spyware

Watches quietly and reports back — browsing, files, credentials. Stealth is the whole point.

Keylogger

Records keystrokes. A subtype of spyware; can also be a hardware dongle inline with the keyboard.

Rootkit

Hides itself and others by subverting the OS at kernel or firmware level. Often needs offline or bare-metal removal.

Backdoor / RAT

Keeps a remote channel open for the operator, bypassing normal authentication.

Bot / botnet

Enrols the host in a controlled fleet — DDoS, spam, crypto-mining, proxying. The victim is the resource.

Logic bomb

Dormant code that fires on a condition — a date, or an employee record disappearing. Classic insider tool.

Fileless

Lives in memory using built-in tools — PowerShell, WMI, registry. Leaves no file for signatures to match.

Adware / PUP

Injects ads or bundles unwanted software. Often technically consented to, buried in an installer.

Where people lose the mark

Three distinctions that decide most malware questions.

Spread vs payload

Virus, worm and trojan describe **how it arrives**. Ransomware and spyware describe **what it does**. A trojan that drops ransomware is both — the two axes are not alternatives.

Worm vs virus

Both replicate — that is why they get confused. The tell is **user interaction**: a worm needs none, a virus needs someone to run the host file.

Rootkit vs backdoor

A backdoor grants **access**; a rootkit grants **invisibility**. Rootkits usually contain a backdoor, but the defining trait is concealment.