PART A – READING COMPREHENSION - (0,75 each question)

TEXT A	TEXT B
‘It’s quite feasible to start a war’: just how dangerous are ransomware hackers? By Sirin Kale	There’s a Better Way to Stop Ransomware Attacks By Paul Rosenzweig
They have the sort of names that only teenage boys or aspiring Bond villains would dream up (REvil, Grief, Wizard Spider, Ragnar), they base themselves in countries that do not cooperate with international law enforcement and they don’t care whether they attack a hospital or a multinational corporation. Ransomware gangs are suddenly everywhere, seemingly unstoppable – and very successful. The gangs – criminal enterprises that hack into internet-connected computer systems, lock access to them, and then sell a decryption key in exchange for payment in bitcoin – have targeted schools, hospitals, councils, airports, government bodies, oil pipelines, universities, nuclear contractors, insurance companies, chemical distributors and arms manufacturers. Hackers haven’t targeted air traffic controllers yet, but some believe that it’s only a matter of time. All organisations are vulnerable, although a sweet spot is mid-size businesses that have enough revenue to make them a lucrative target, but aren’t large enough to have dedicated cybersecurity teams. “Everybody who uses internet-connected computer systems has vulnerabilities,” says Dr Herb Lin, a cybersecurity expert at Stanford University. Russia is a major hotspot for ransomware attackers to headquarter themselves, as is Iran. Cyrillic – the Russian alphabet – is commonly used in ransomware forums or source codes. “It’s not that the Russian government is conducting these ransomware attacks,” Lin says, “but they have an arrangement in which the Russian-based cyber-mobs can do their activities outside Russia, and the country turns a blind eye to it. These hackers operate as organised gangs: some members specialise in identifying compromised systems and gaining access, while others handle the ransom negotiations. (Investigators tracing ransom payments will often see cryptocurrency transferred into many different cyberwallets after a transaction has been made, for this reason.) https://www.theguardian.com/technology/2021/aug/01/crypto-criminals-hack-the-computer-systems-of-governments-firms-even-hospitals	Ransomware attacks are plaguing the United States. With alarming regularity, cybercriminals disrupt computer systems controlling important pieces of infrastructure and refuse to restore access until they are paid — typically in Bitcoin or another decentralized, hard-to-trace cryptocurrency. The Biden administration has taken some steps to address the problem. An executive order in May directed the federal government to enhance coordination on the issue. A national security memorandum in July outlined better security standards for America’s industrial control systems. But none of these efforts tackle the problem at its root. Ransomware attacks occur because criminals make money from them. If we can make it harder to profit from such attacks, they will decrease. The United States can make it harder. By more aggressively regulating cryptocurrencies, the government can limit their use as an anonymous payment system for unlawful purposes. In the nonvirtual world, kidnappings for ransom are wildly unsuccessful. Between 95 percent and 98 percent of criminals involved in cases of kidnapping for ransom that are reported to the police are caught and convicted. Why? In part because at the moment when the victims are exchanged for cash, the criminals put themselves at great risk of identification and capture. Ransomware attacks are different. Cybercriminals can “kidnap” a company from afar and receive payment anonymously and securely in the form of cryptocurrency. (Technically, cryptocurrency use is only pseudonymous, but in practice the challenge of identifying a user is formidable.) https://www.nytimes.com/2021/08/31/opinion/ransomware-bitcoin-cybersecurity.html?searchResultPosition=4

Read the two excerpts below carefully and answer the questions

There is information about the region or regions responsible for the highest number of attacks. Identify this information and choose the correct answer.

R: Text A – Two regions responsible

Where can we find the main reason for the growth of this type of attack?

R: Only on Text B

The structure of these hackers is like the organized crime with experts in each part of the process. We can find this information:

R: Only on Text A

The main difficulty in arresting these hackers has a direct relationship with cryptocurrencies. This information is:

R: In both texts

PART B – Linguistic Elements – (0,60 each question)

Choose the best option for completing the sentence:

The anonymous, poorly regulated nature of cryptocurrency provided tinder for the ransomware fire. At some point, we _____ depriving the inferno of fuel.

R: may have to consider

Choose the best option for completing the sentence:

Hackers got in through a password belonging to a third-party vendor that _____ and _____ on the dark web.

R: had been breached / sold

What is the anthonym of feasible in this sentence: “It’s quite **feasible** to start a war”

R: Unviable

Choose the best synomym for the word "*ransom*" according to the sentence:

"*Some organizations are tempting targets because they seem more likely to pay a ransom quickly."*

R: Payoff

Read the excerpt and choose the best synonym for "*flair"* and *"snarky*" respectively according to the text.

*Each group has a distinct character. "REvil has some **flair**, as does Pysa, who are quite **snarky**," says Brett Callow of the cybersecurity firm Emsisoft. "At the other end of the spectrum, Ryuk are robotic in their approach."*

R: Talent - Sarcastic

PART C – Writing

Explain why is so difficult to control ransomware attacks? (at least 5 lines – 1,50)

Do you think ransomware attacks are a problem that should be solved only by affected sectors or should governments act to control these attacks and protect the population? Justify your opinion. (at least 10 lines – 2,50)