French blood fridges hit by cyber-attacks

LEVEL B2


Photo: Léonard Cotte / Unsplash

I. WARM-UP

1. Which systems are most critical to keep online in your city?
2. What signs tell you a website or device may be unsafe?
3. Should companies report cyber-attacks immediately? Why or why not?

II. KEY VOCABULARY

hack
To break into a computer system without permission.

culprit
A person or group believed to be responsible for a problem or crime.

honeypot
A fake system set up to attract hackers so experts can study them.

decoy
Something that looks real but is used to trick and draw in attackers.

co-ordinate
To organise actions so they happen together effectively.

intervene
To step in and take action to prevent harm or change a result.

probe
To test or examine something carefully to find weaknesses or information.

attribution
The act of naming who carried out an attack or action.

III. READING

France's Blood Establishment (EFS) said hackers had targeted cold rooms for donated blood and tried to raise their temperatures. Staff intervened quickly, and EFS reported no health impact or loss of blood. Until then, only supermarkets were known to be hit.

Online, Noname057(16) and the Z-Pentest Alliance claimed they hacked Danfoss, a maker of freezer controllers, leading some to call them the culprits. Analysts doubt the link, and say Russian or Iranian hacktivists, state actors, or even teenagers could be responsible.

To study the attacks, three cyber-security firms deployed honeypots — decoy freezer software — to watch how intruders probe systems. Sekoia noted similar scanning, but said it might be automatic.

Its report to clients said the pattern aligned with Russian "hybrid warfare", yet also pointed to Iranian-aligned actors and cited about 40 Israeli supermarkets hit in 2022. It also noted US military base freezers were forced into defrost in late August, though models are unconfirmed and investigations are ongoing.

Ryan Dewhurst of Previdian said simultaneous, overnight temperature changes showed the attack was planned and co-ordinated, using weak entry points already known online. Authorities are investigating, but no formal attribution has been made.

Reading text adapted from reporting by **BBC News***: "French blood storage impacted by freezer hacks...". Original article linked at theenglishwire.com.*

IV. COMPREHENSION QUESTIONS

1. What did EFS say hackers tried to do to its blood storage?
2. How did staff respond, and what was the result?
3. Which groups claimed online that they hacked Danfoss?
4. How did researchers safely observe the attackers' methods?
5. What did Ryan Dewhurst conclude about the nature of the attacks?

V. DISCUSSION

1. Should firms name suspects before formal attribution? Why or why not?
2. Who should secure critical equipment like medical fridges?
3. Are honeypots an ethical and effective defence tool? Explain.
4. Which basic settings make internet-linked devices harder to hack?

VI. GRAMMAR FOCUS

Past perfect continuous

Use had been + verb-ing to show an action in progress up to an earlier past point. Common cues: before + past event, by then, until then, for + time, since + point.

"By then, attackers **had been scanning** *European systems for days."*

"Before staff intervened, hackers **had been trying** *to raise temperatures."*

VII. GRAMMAR EXERCISE

Complete each sentence with the past perfect continuous form.

1. A fridge (run) ___ for years when hackers found it online. _____
2. She was tired because she (study) ___ the attack for hours. _____
3. Until then, firms (watch) ___ honeypots for days. _____
4. By the time alerts came, bots (probe) ___ traps for days. _____
5. Before the response, groups (plan) ___ attacks for some time. _____

Teacher's Notes

TEACHERS ONLY

These notes are designed to help you get the most out of this lesson. Please do not share this page with students.


Photo: Léonard Cotte / Unsplash

I. LESSON GUIDE

- Timing: 8–10 minutes warm-up, 10 minutes vocabulary, 12–15 minutes reading and comprehension, 8–10 minutes grammar, 10–12 minutes discussion.
- Pre-teach or check: hack, honeypot, decoy, co-ordinate, intervene, attribution. Use quick examples from the text.
- Run a first silent read for gist, then a second for detail with pair-checks before open class. The topic involves security and possible blame; keep discussion on public systems rather than students' private accounts if anyone seems uncomfortable.
- Differentiation: stronger students summarise the positions of the analysts, Sekoia and Dewhurst; others underline evidence in the text and match it to those views.

II. DISCUSSION FACILITATION TIPS

1. Start with a quick show of hands, then pair students with different views to swap reasons.
2. Elicit concrete tasks (updating, monitoring, funding) and who should do each one.
3. Prompt pros (insight) and cons (risk, legality). Ask for one example of each.
4. Board a short list first (strong passwords, updates, 2FA), then have students add one more.

III. EXTENSION ACTIVITIES

Debate: In teams, prepare a 90-second argument for or against publicly naming suspects before attribution.

Research: Pairs create a one-slide brief on honeypots: purpose, one risk, and one real insight from the text.

IV. ANSWER KEY OVERVIEW

Comprehension questions: short factual answers from the text.

Grammar exercise: Past perfect continuous

Discussion: open-ended. Accept any reasonable ideas supported by examples and reasoning.

Answer Key

TEACHERS ONLY

These answers are for teachers only. Please do not share this page with students.


Photo: Léonard Cotte / Unsplash

IV. COMPREHENSION QUESTIONS

1. What did EFS say hackers tried to do to its blood storage?
   They tried to raise temperatures in EFS cold rooms for blood.
2. How did staff respond, and what was the result?
   They intervened quickly, and there was no health impact or loss of blood.
3. Which groups claimed online that they hacked Danfoss?
   Noname057(16) and the Z-Pentest Alliance.
4. How did researchers safely observe the attackers' methods?
   They used honeypots, decoy freezer software, to watch how hackers probe systems.
5. What did Ryan Dewhurst conclude about the nature of the attacks?
   They were planned and co-ordinated, with simultaneous overnight changes.

V. DISCUSSION

Open answers. Accept any reasonable ideas supported by examples and reasoning.

VI. GRAMMAR FOCUS

Key point: Use had been + verb-ing to show an action in progress up to an earlier past point. Common cues: before + past event, by then, until then, for + time, since + point. (Examples constructed.)

"By then, attackers **had been scanning** *European systems for days."*

"Before staff intervened, hackers **had been trying** *to raise temperatures."*

VII. GRAMMAR EXERCISE

Complete each sentence with the past perfect continuous form.

1. A fridge ___ for years when hackers found it online. **had been running**
2. She was tired because she ___ the attack for hours. **had been studying**
3. Until then, firms ___ honeypots for days. **had been watching**
4. By the time alerts came, bots ___ traps for days. **had been probing**
5. Before the response, groups ___ attacks for some time. **had been planning**