



| Flash |

French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Cyberattack, Retail, Geopolitical, France

October 15, 2026

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP: CLEAR

Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 6:30 AM (EDT) on October 14, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

| Key Findings

- ZeroFox assesses the October 11–12 cyberattack on French supermarket refrigeration systems is consistent with pro-Russia cyber techniques used against European states supporting Ukraine; no actor has claimed responsibility, and attribution remains unconfirmed.
- The attack is suspected to have exploited previously disclosed vulnerabilities in end-of-life or outdated Danfoss AK-SM 800A refrigeration controllers, including flaws that could allow authentication bypass and remote code execution (RCE).
- The attack occurred amid civil unrest that Russia-linked influence operations are almost certainly already exploiting.
- Organizations operating internet-exposed, end-of-life, or outdated Danfoss refrigeration controllers face elevated risk of similar attacks.

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP: CLEAR

| Details

ZeroFox assesses the October 11–12 cyberattack on French supermarket refrigeration systems is consistent with pro-Russia cyber tactics used against European states supporting Ukraine; no actor has claimed responsibility, and attribution remains unconfirmed as of writing. Attackers reportedly raised temperatures to as high as 122°F (50°C), causing fires, destroying food stocks, and forcing some refrigeration equipment to be taken offline. The financial loss is estimated to be tens of millions of euros. The attack is suspected to have been enabled by vulnerabilities in Danfoss AK-SM 800A refrigeration controllers.¹

- Danfoss is a Danish engineering company providing Heating, Ventilation, and Air Conditioning (HVAC) technology, among other industrial automation technologies.
- Danfoss control systems manage critical refrigeration functions such as temperature, evaporators, compressors, condensers, and defrost cycles in various settings, including those in supermarkets and cold storage facilities.

The affected controllers were likely at end-of-life or running outdated firmware, though it is unclear which versions enabled the attack. Researchers have observed multiple vulnerabilities in Danfoss refrigeration controllers, including flaws that could allow attackers to bypass authentication and execute code on affected devices.²

- Most affected equipment is reportedly legacy hardware that no longer receives security updates, and some AK-SM 800A units on outdated firmware were also hit.³

ZeroFox cannot determine whether the majority of the concentration of impact in France, at the time of writing, reflects deliberate targeting or exposure. Danfoss has a global customer base, but a large share of internet-exposed Danfoss interfaces are in France.

¹ [hXXps://www.reuters.com/business/retail-consumer/french-supermarket-chain-intermarche-hit-by-cyberattack-150-stories-targeted-2026-10-12/](https://www.reuters.com/business/retail-consumer/french-supermarket-chain-intermarche-hit-by-cyberattack-150-stories-targeted-2026-10-12/)

² *Ibid.*

³ [hXXps://www.afp.com/en/french-supermarkets-suffer-refrigerator-shutdown-after-unprecedented-cyberattack](https://www.afp.com/en/french-supermarkets-suffer-refrigerator-shutdown-after-unprecedented-cyberattack)

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP: CLEAR

- At least one retail employee reportedly said all stores monitored by the Danfoss central platform were hit, which likely points to a shared management path rather than store-by-store targeting.⁴

The attack method matches pro-Russia hacktivist techniques used against exposed operational technology (OT). A December 2025 advisory from the Cybersecurity and Infrastructure Security Agency (CISA) assessed that groups such as NoName057(16), Cyber Army of Russia Reborn (CARR), Z-Pentest, and Sector 16 exploit minimally secured internet-facing devices to gain access to the OT of critical infrastructure, with impacts that include physical damage.⁵

- Several Western Intelligence and law enforcement agencies link many of these groups to Russian state entities.⁶
- In January 2026, pro-Russia actors claimed a distributed denial-of-service (DDoS) attack against Danfoss over Denmark's military support for Ukraine.⁷

⁴ [hXXps://techaiwire\[.\]com/articles/french-supermarket-cyberattack-danfoss-refrigeration/](https://techaiwire[.]com/articles/french-supermarket-cyberattack-danfoss-refrigeration/)

⁵ [hXXps://www.cisa\[.\]gov/news-events/alerts/2025/12/09/opportunistic-pro-russia-hacktivism-attack-us-and-global-critical-infrastructure](https://www.cisa[.]gov/news-events/alerts/2025/12/09/opportunistic-pro-russia-hacktivism-attack-us-and-global-critical-infrastructure)

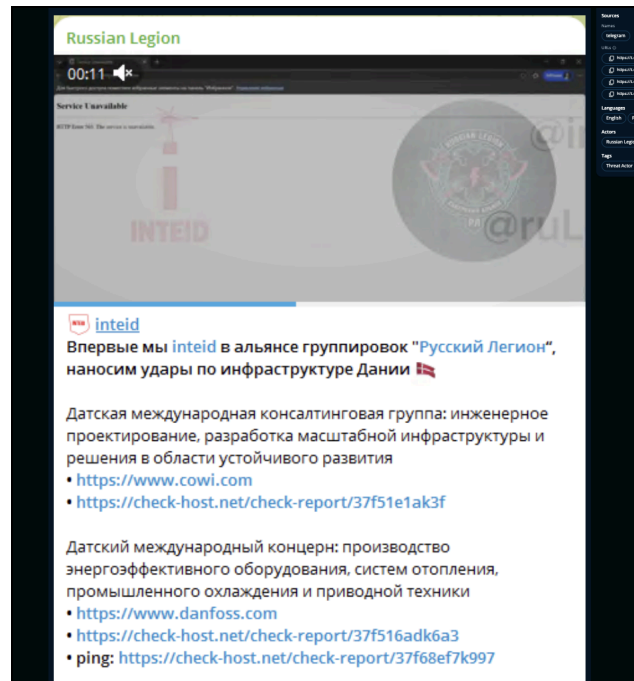
⁶ [hXXps://www.ic3\[.\]gov/CSA/2025/251209.pdf](https://www.ic3[.]gov/CSA/2025/251209.pdf)

⁷ https://cloud.zerofox.com/intelligence_new/advanced_dark_web/99356

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP: CLEAR



Pro-Russia actors claiming a DDoS attack against Danfoss on Telegram

Source: ZeroFox Intelligence

The attack occurred amid civil unrest across France, which began in late September as student protests over school conditions near Paris and spread nationwide.

- As of October 9, France's Ministry of Justice reported 6,877 arrests since the movement began (with 86 percent involving minors), and authorities reported 761 police officers and gendarmes injured.⁸
- Several schools have been damaged, burned, or ransacked, and student blockades were still under way on October 9, two days before the supermarket attacks.⁹

Although attribution for the French refrigerator system attacks remains unconfirmed, multiple European governments have warned of Russian hybrid operations, including

⁸ [hXXps://euronews\[.\]com/2026/10/11/teen-revolt-or-revolution-the-student-protests-threatening-frances-presiden](https://euronews.com/2026/10/11/teen-revolt-or-revolution-the-student-protests-threatening-frances-presidential-race)
tial-race

⁹ [hXXps://www.france24\[.\]com/en/france/20261001-hundreds-of-students-detained-dozens-of-officers-injured-in-](https://www.france24.com/en/france/20261001-hundreds-of-students-detained-dozens-of-officers-injured-in-french-school-protests)
french-school-protests

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP: CLEAR

cyberattacks, against states supporting Ukraine.¹⁰¹¹¹² According to a U.S.-based information-reliability firm that tracks online misinformation, likely Russia-sponsored misinformation has been identified in connection with the ongoing unrest in France.¹³

- Pro-Russia actors targeted Danfoss in January 2026, and groups linked to Russian state entities have been documented exploiting exposed OT for physical effects.¹⁴¹⁵
- A Russian influence campaign circulating fake stories imitating legitimate outlets has also ramped up during the unrest.¹⁶

Threat actors often target HVAC systems, as they commonly connect to the corporate networks of the organizations and are typically less defended than the network itself, enabling operational disruption, lateral movement, or both. In the past 90 days, ZeroFox has observed ransomware and extortion leak sites targeting at least 20 HVAC-related victims, 17 of which are based in the United States.

- We observed threat actors attacking all layers of the HVAC supply chain, including installers, mechanical contractors, equipment and component manufacturers, and distributors.
- The top five threat actors observed targeting HVAC-related entities in the past 90 days were ransomware groups Qilin, SafePay, DragonForce, Akira, and Storm.

¹⁰ [hXXps://www.bbc.com/news/articles/c60rl5vwpk02o](https://www.bbc.com/news/articles/c60rl5vwpk02o)

¹¹ [hXXps://www.europarl.europa.eu/news/en/press-room/20260911IPR47452/the-european-parliament-demands-a-firmer-eu-response-to-hybrid-threats](https://www.europarl.europa.eu/news/en/press-room/20260911IPR47452/the-european-parliament-demands-a-firmer-eu-response-to-hybrid-threats)

¹² [hXXps://www.bbc.com/news/articles/c60rl5vwpk02o](https://www.bbc.com/news/articles/c60rl5vwpk02o)

¹³ [hXXps://www.newsguardrealitycheck.com/p/in-france-real-protests-distorted](https://www.newsguardrealitycheck.com/p/in-france-real-protests-distorted)

¹⁴ http://cloud.zerofox.com/intelligence_new/advanced_dark_web/99356

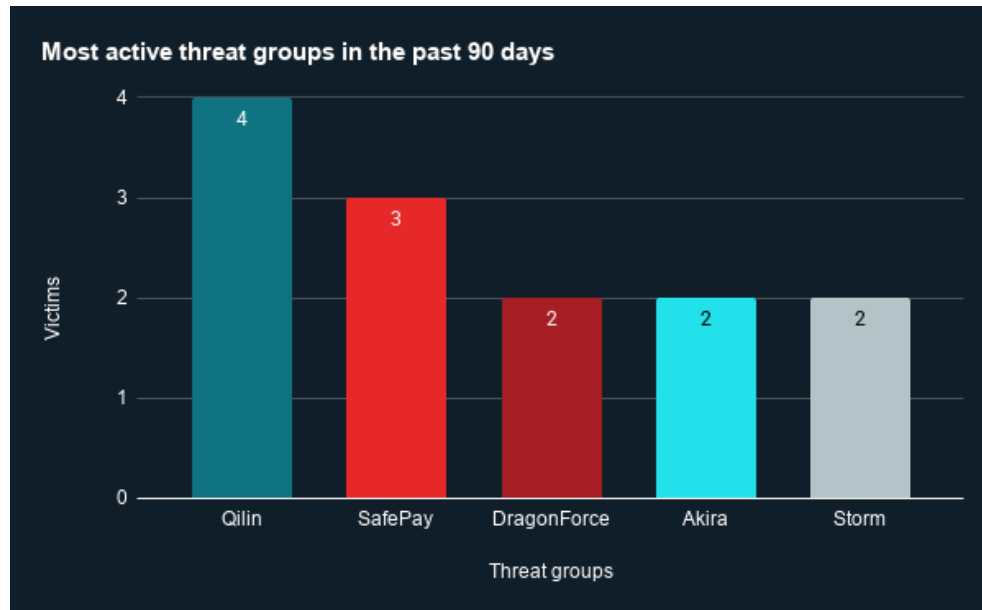
¹⁵ [hXXps://www.ic3.gov/CSA/2025/251209.pdf](https://www.ic3.gov/CSA/2025/251209.pdf)

¹⁶ [hXXps://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/october/French-student-protest/](https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/october/French-student-protest/)

Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP: CLEAR



Top five threat groups observed targeting HVAC systems in the last 90 days

Source: ZeroFox Intelligence

Organizations operating internet-exposed, end-of-life, or outdated Danfoss controllers face elevated risk of similar attacks. Danfoss stated it had already advised supermarkets to move off the legacy models that no longer receive security updates.¹⁷

- On October 12, France's Computer Emergency Response Team (CERT-FR) advised operators to disconnect AK-SM and AK-SC controllers or tightly filter access.
- As controller-based alarms reportedly failed or lagged in some stores, ZeroFox recommends utilizing independent temperature sensors with their own alerting for a second layer of warning.

¹⁷ <https://www.reuters.com/legal/litigation/investigators-hunt-french-supermarket-fridge-hackers-no-claim-responsibility-2026-10-13/>

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a

TLP:CLEAR

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Flash | French Supermarket Cyberattack amid Civil Unrest Consistent with Pro-Russia Cyber Tactics

F-2026-10-15a
TLP: CLEAR

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%