Container Store Restores Systems After Cyberattack Linked to n0n Claims

The Container Store says its website and systems are restored after a weekend incident that disrupted online ordering and in-store payments. The n0n extortion group listed the firm on its leak site; the company has not addressed that claim.

- The incident disrupted online ordering and forced stores to use alternative transaction-processing procedures, though stores stayed open.
- The parent company, Neighborhood Intelligence, says only The Container Store was affected, not its other brands.
- It does not appear customer financial data was stolen, but the company did not respond to n0n's leak-site claim.
- n0n emerged in September, focuses on ransomware and data extortion, and has reportedly hit more than 100 organizations.
- LevelBlue says the group used AI coding tools to write and debug attack scripts.

The Container Store, a US home-storage retailer with about 100 stores, has said it restored its website and systems after a cybersecurity incident over the previous weekend. The incident shut down online ordering and limited in-store transaction processing. Stores stayed open by using alternative procedures.

What is known

The parent company, Neighborhood Intelligence, says the incident affected only The Container Store and not its other brands. It hired cybersecurity experts to contain the incident and restore systems. So far it does not appear that customer financial data was stolen. The company did not address claims by the n0n group, which listed it on its leak site earlier this month.

About n0n

According to the source, n0n emerged in September and specializes in ransomware and data extortion. It is said to have attacked more than 100 organizations and demanded ransoms running into hundreds of millions of dollars. SOCradar reports that the group moved from charging victims a 10% fee for access to its

negotiation portal to requiring full payment before showing any sample of stolen data. Recorded Future's Allan Liska says affiliates were told to target only companies earning above $10 million a year. LevelBlue says the group mainly targets healthcare and pharmaceuticals but has recently claimed data from financial services and retail firms, and that it uses AI coding tools to scale its operations.

Why it matters

The case shows that an extortion incident can disrupt payments and ordering even when stores keep trading, and that a restored system does not settle questions about data. For regulated institutions, the practical lesson is to prepare for degraded operations and to be ready to assess leak-site claims.

What to do now

1. Test manual or alternative payment and order-handling procedures so core services continue if systems are disrupted.
2. Define a process to verify and triage claims that your organization or a supplier appears on a ransomware leak site.
3. Review business continuity plans against SAMA BCM and NCA ECC expectations, including recovery time targets for payment systems.
4. Confirm that incident response retainers and escalation paths to regulators are current, including PDPL breach-notification duties.
5. Check third-party and retail-partner exposure, and ensure data held by suppliers is covered by contract security terms.