# n0n Group Puts Dozens of Global Ports and Shipping on Its Leak Site

By Omer Faruk Diken

Published: 2026-10-13 · Archived: 2026-11-17 02:00:57 UTC

A month after its first leak site postings, the n0n extortion group has turned its attention to global shipping. On October 12, 2026, the group added 38 organizations to its Dark Web leak site in one batch: container terminals in Brazil, Spain, Morocco, India and Vietnam, shipping lines in Singapore, China and Taiwan, port IT providers in Kuwait, Indonesia and Germany, and a dense cluster of South Korean operators.

The batch more than doubles the group's public victim count and shifts it from an opportunistic, cross-sector actor to one with a clear sector focus. The way the stolen data is described also raises a question that matters more to the maritime industry than any single listing: whether these are 38 separate intrusions, or exposure flowing out of one shared system.

## Key Takeaways

- **Actor:** n0n is a financially motivated data-theft extortion group that emerged in September 2026
- **Maritime wave:** On October 12, 2026, n0n posted 38 organizations in a single batch, nearly all in port, shipping and logistics, across 18 countries
- **Concentration:** South Korea accounts for 12 of the 38 entries, including Busan terminal operators BNCT and Pusan Newport Company
- **Likely shared entry point:** Small, application-scoped data sets and incomplete infostealer coverage across victims point to an exposed shared application or vulnerability rather than separate intrusions
- **Deadline and demands:** The maritime entries are set to publish on October 19, 2026, at 13:27 UTC, with reviewed demands ranging from USD 2.4 million to USD 14 million
- **Verification:** None of the maritime claims had been publicly confirmed by a listed organization at the time of writing

## n0n at a Glance

| Attribute | Detail |
|---|---|
| Name | n0n |
| Type | Data-theft extortion group |
| First seen | September 2026 |
| Source country | Likely Russia |

| Attribute | Detail |
|---|---|
| Initial access | Likely a shared application or vulnerability |
| Victims before the maritime wave | 21 (as of October 8, 2026) |
| Maritime wave | 38 organizations posted on October 12, 2026 |
| Maritime publication deadline | October 19, 2026, 13:27 UTC |
| Status | Active |

## Who Is n0n?

n0n is a financially motivated extortion group that emerged in September 2026 and monetizes stolen data through public leak postings. SOCRadar's tracker profile describes an operation that gets in with credentials harvested by infostealer malware, exfiltrates material such as Active Directory mappings and legal documents, and then pressures victims with Dark Web leak postings.

The profile also notes that n0n avoids traditional ransomware deployment and instead manipulates victim data with administrative tools. Its ATT&CK mapping still includes encryption and recovery-inhibition techniques, so defenders should not rule out disruptive impact.

Until an encryptor is publicly tied to the group, n0n is best treated as a data-theft extortion operation with the access to cause damage.

Before the maritime wave, n0n's victimology was broad and opportunistic. Its first 21 listings spanned investment firms, telecommunications, retail, education and pharmaceuticals across 17 countries, including claims against Fanatics, Transcom WorldWide, AstraZeneca Türkiye, Argentina's Ministry of Education, STOKR and Venezuelan internet provider Inter. SOCRadar rates n0n near the top of its aggressiveness scale and near zero for lethality.

## Inside the October 12 Maritime Wave

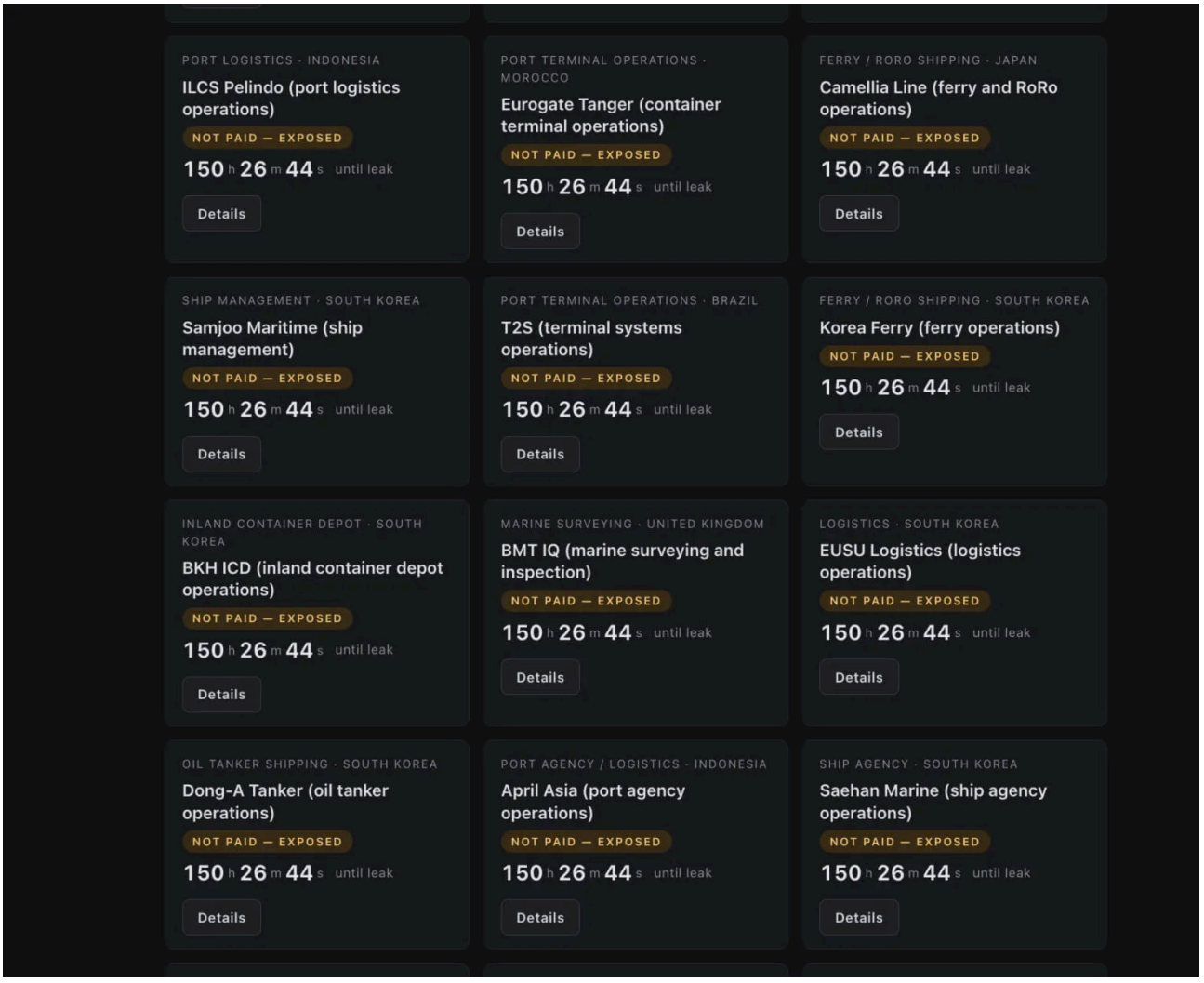
The 38 organizations posted on October 12 cover almost every link in the container supply chain, from the terminal gate to the shipping line, the port agent and the IT systems that connect them.

| Segment | Organizations |
|---|---|
| Container terminals and port operators | Santos Brasil, Portonave and Superterminais (Brazil); Asyaport (Turkey); MGNP, BNCT and Pusan Newport Company (South Korea); TTI Algeciras (Spain); Eurogate Tanger (Morocco); NCT Kandla (India); Nam Dinh Vu Port (Vietnam); NEOM Ports (Saudi Arabia) |
| Port IT, EDI and terminal systems | GNCNet / DGT Busan (South Korea); GCS Kuwait (Kuwait); ILCS Pelindo (Indonesia); HPC Hamburg Port Consulting (Germany); T2S (Brazil) |

| Segment | Organizations |
|---|---|
| Shipping lines and ship operators | Ocean Network Express (Singapore); CULines (China); T.S. Lines (Taiwan); Polaris Shipping, Dong-A Tanker, Samjoo Maritime and Korea Ferry (South Korea); Camellia Line and Tsuneishi / Kambara Kisen (Japan); Samudera (Indonesia) |
| Agencies, logistics, depots and surveying | Saehan Marine, EUSU Logistics and BKH ICD (South Korea); April Asia and GlobalNet LCL (Indonesia); Yusen Logistics Hong Kong; Premier Alliance (Netherlands); BMT IQ (United Kingdom) |
| Adjacent industry | ZPMC (China); Apical Group (Singapore); Dongkuk Steel (South Korea) |

South Korea, with 12 entries spanning terminal operators, a Busan port IT provider, ship agents, an inland container depot and Korean shipping companies. SOCRadar's South Korea Threat Landscape Report found ransomware targeting in the country weighted toward finance, insurance and manufacturing, which makes a maritime cluster of this size stand out. Another interesting point is the presence of five port IT and terminal systems providers, organizations whose business is holding other companies' operational data.

The posts follow a fixed format. Each names the organization with its function in brackets, gives its segment and country, summarizes the claimed data in one line, and closes with a "NOT PAID, EXPOSED" status and a countdown to publication.

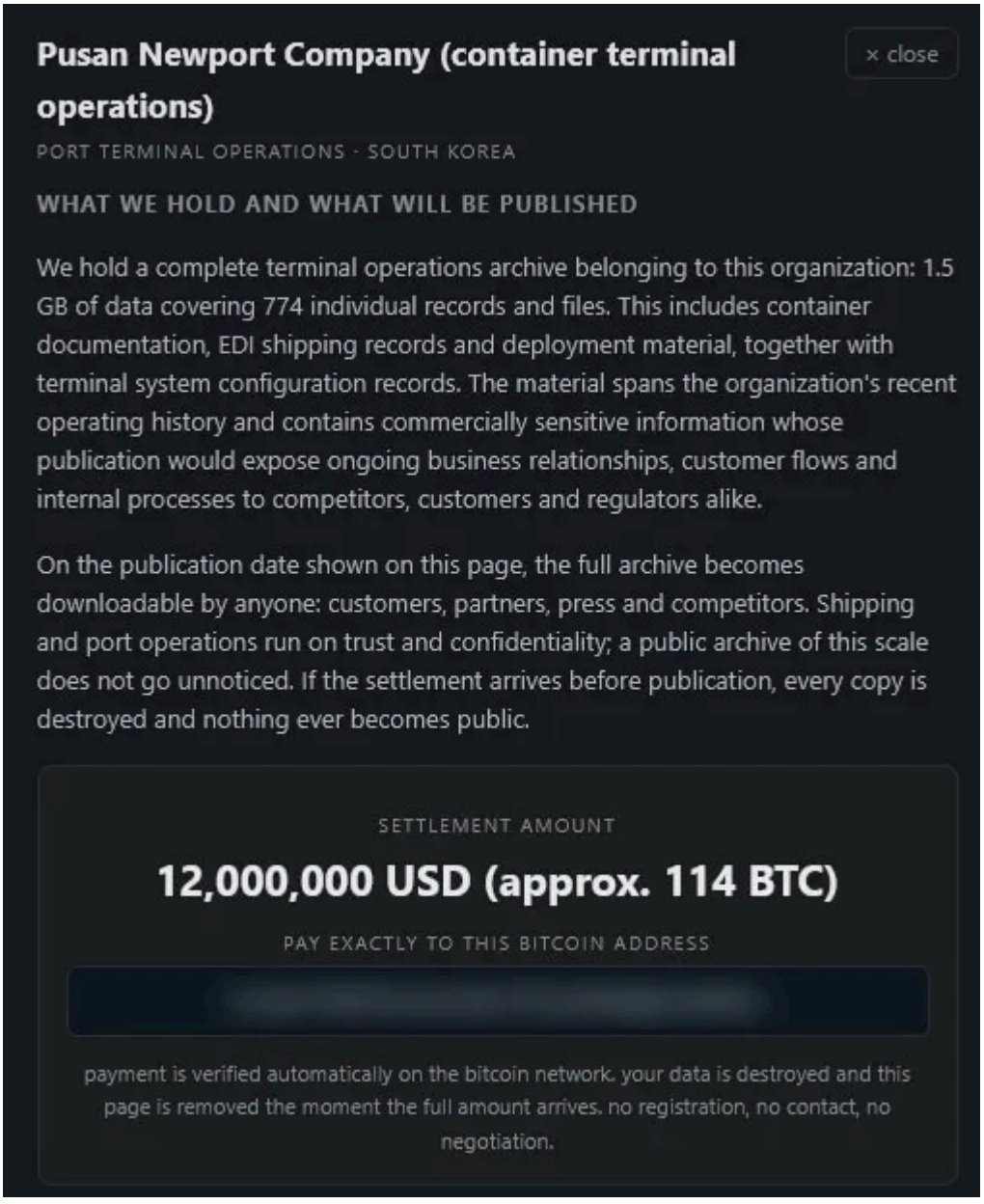



*Maritime and logistics victims on n0n's Dark Web leak site, each marked "NOT PAID, EXPOSED" with a countdown to publication*

The detail pages behind the maritime listings point to one exposed application or vulnerability rather than 38 separate network intrusions. Reviewed postings  describe small, narrowly scoped data sets:

| Organization | Claimed volume | Files | Data described |
|---|---|---|---|
| Nam Dinh Vu Port | Not stated | 23,507 EDI message files | Vessel schedules, container manifests, gate movement records and booking messages exchanged with multiple international shipping lines |
| ILCS Pelindo | 2.4 GB | 108 | EDI container manifest archives and operational records |
| Pusan Newport Company | 1.5 GB | 774 | Container documentation, EDI shipping records, deployment material and terminal system configuration records |

| Organization | Claimed volume | Files | Data described |
|---|---|---|---|
| Eurogate Tanger | 660 MB | 354 | Commercial configuration records, systems release documentation, and container and vessel records |
| BMT IQ | 90 MB | 18 | Commercial e-invoice records, equipment interchange receipts and inspection records |
| EUSU Logistics | 60 MB | 41 | Infrastructure configuration and assessment records and internal systems material |




*n0n's posting for Pusan Newport Company claims 1.5 GB of container documentation, EDI shipping records, deployment material and terminal system configuration records*

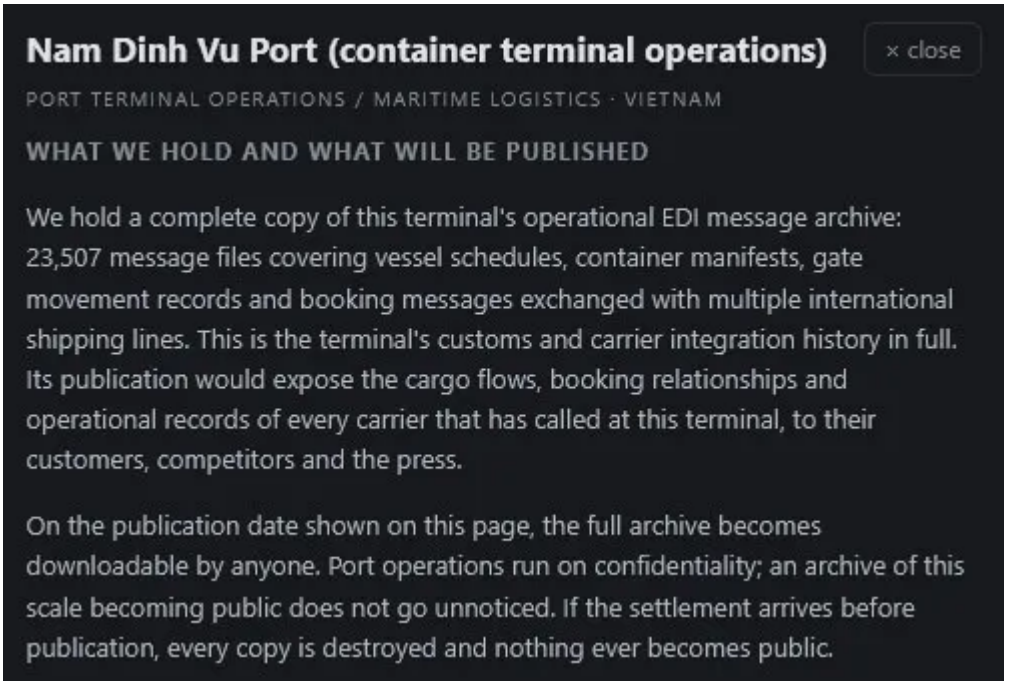
Three observations support a shared entry point:

- **Scale:** Each reviewed listing presents its data as a complete archive or copy, yet volumes run from 60 MB to 2.4 GB and file counts from 18 to 774, the footprint of a single application's data store rather than a compromised corporate network
- **Content:** The same narrow categories recur across countries and business types: EDI messages, manifests, gate and equipment interchange records, terminal system configuration, release documentation and deployment material
- **Access:** SOCRadar checks stealer-log data for n0n victims' domains, and did not find credential matches for many maritime organization listed, so stolen credentials, n0n's documented entry point, do not explain the batch

Release documentation and deployment material sit with the systems and integration layer that connects terminals, carriers and agents. The likeliest source is therefore a platform that many of these organizations use or exchange data through, such as a terminal system, EDI integration or file transfer product, reached through a vulnerability or a shared access path.

The pattern resembles earlier mass-exploitation extortion campaigns, such as those against MOVEit Transfer in 2023 and Cleo in 2024, where a flaw in one widely deployed file transfer product produced a long list of victims whose data came from that single application. There is no evidence linking n0n to those campaigns.

A shared source also widens the exposure beyond the 38 names. The Nam Dinh Vu Port posting itself states that its archive would expose the cargo flows, booking relationships and operational records of every carrier that called at the terminal. Interchange headers in any published EDI files, together with archive date ranges, should help identify the system the data came from.




*n0n's posting for Nam Dinh Vu Port describes an archive of 23,507 EDI message files exchanged with multiple international shipping lines*

## How n0n Applies Pressure

n0n's leak site works as a public scoreboard. Every entry carries a status and a countdown, and the statuses tell victims, and everyone watching, how the group expects negotiations to go.

| Status | What it signals |
|---|---|
| PENDING EXPOSURE | The victim is anonymized as "Company #N" with only a sector and location, and a publication date one to three days out |
| NOT PAID, EXPOSED | The victim is named, with a publication date and countdown |
| HONORED | The victim settled before its deadline; one Canadian financial services company carries this label with a settlement date of October 7, 2026 |

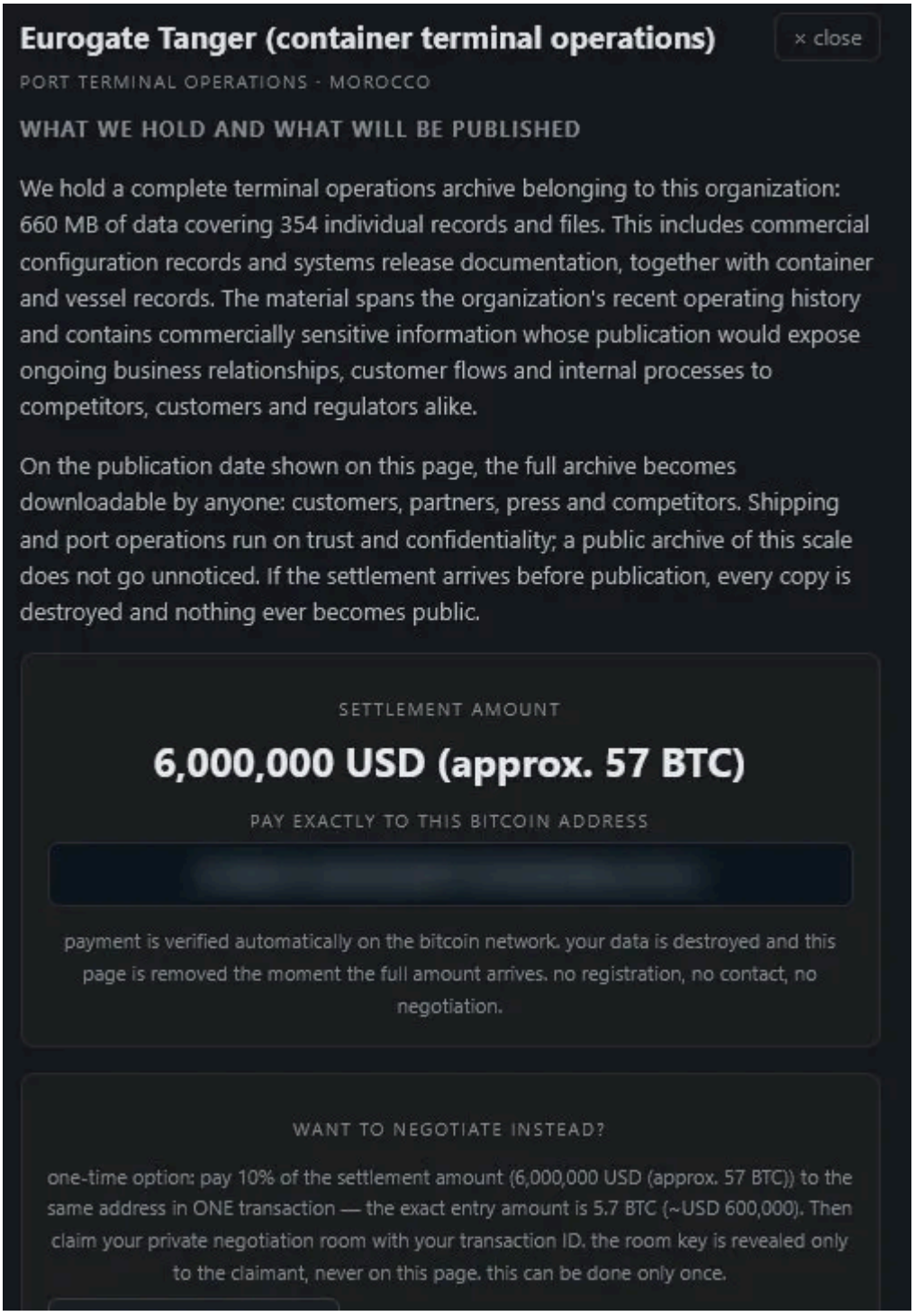
Anonymized posting lets the group show a breach to the victim, and hint at it publicly, while keeping room to negotiate before the name goes out. The "HONORED" label serves the opposite audience: it advertises to future victims that paying works.

The maritime batch breaks from the group's earlier rhythm. Instead of short, staggered deadlines, the maritime entries were posted named and the ones reviewed share a single publication time of October 19, 2026, at 13:27 UTC, a seven-day window. A uniform deadline is consistent with a batch processed at once, which supports the possibility of a common data source discussed above.

### Fixed Prices and a Paid Negotiation Room

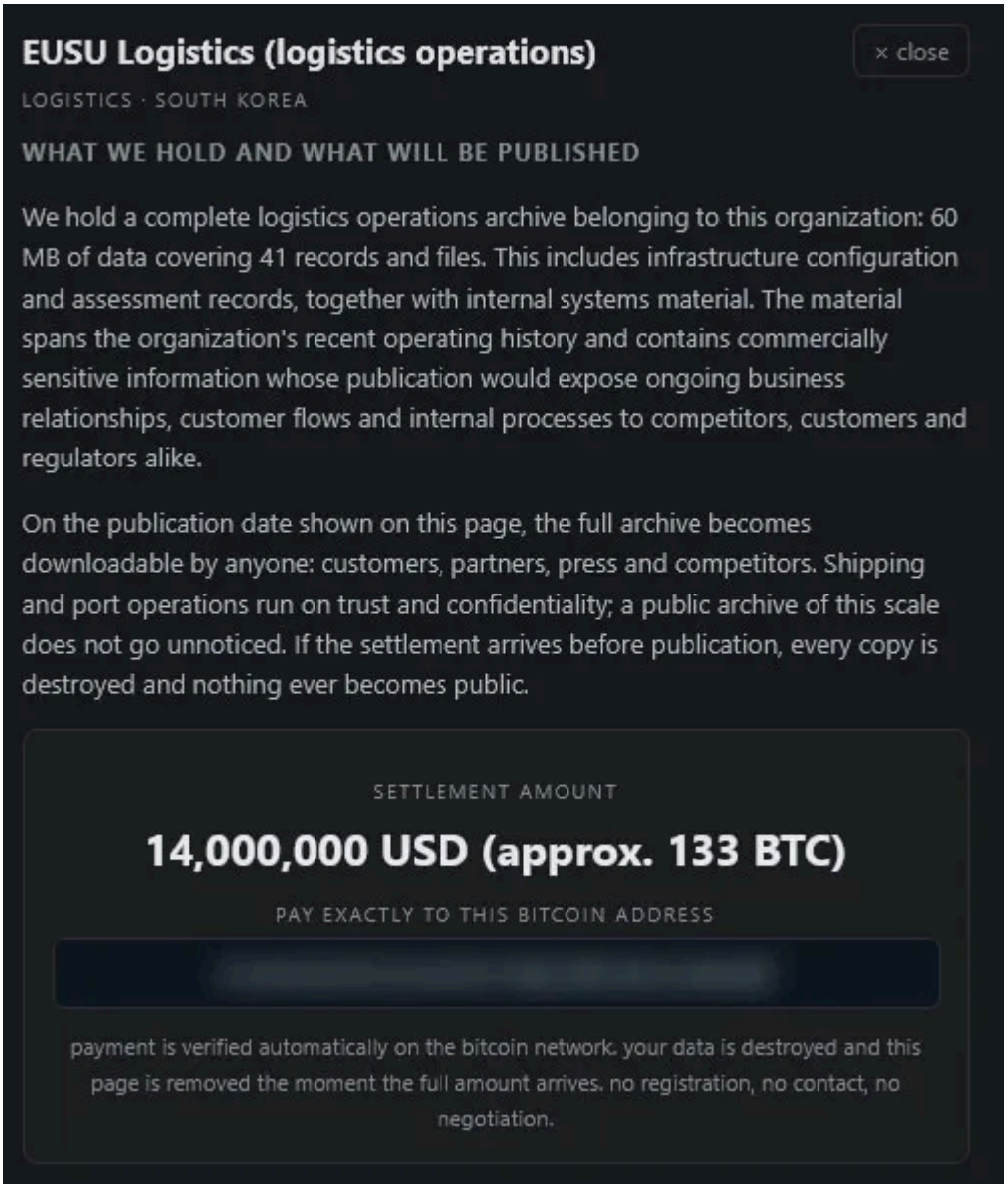
The detail pages reviewed set a fixed settlement amount in US dollars with its Bitcoin equivalent and a dedicated Bitcoin address. The pages state that payment is verified automatically on-chain, and that once the full amount arrives the data is destroyed and the page removed, with no registration, contact or negotiation.

Negotiation is available, at a price. The Eurogate Tanger and ILCS Pelindo pages offer a one-time option: send 10% of the settlement amount to the same address in a single transaction, then use the transaction ID to claim a private negotiation room. For Eurogate Tanger, that entry fee is 5.7 BTC, roughly USD 600,000; for ILCS Pelindo, it is 2.3 BTC, roughly USD 240,000.




*n0n's Eurogate Tanger posting, with a USD 6 million settlement demand and a 10% entry fee for a private negotiation room*

Demands do not scale with data volume. EUSU Logistics faces the highest demand reviewed, USD 14 million for 60 MB of data, while ILCS Pelindo's 2.4 GB carries a USD 2.4 million demand.




*n0n demands USD 14 million from EUSU Logistics for a claimed 60 MB of data*

## How Much Weight Do the Claims Carry?

n0n's claims should be treated as unverified until data is published or a victim confirms. Of the 21 victims SOCRadar tracked before the maritime wave, 19 remain at the "Claimed" stage, one is listed as negotiating and one, Chibitek, has had data leaked.

Several factors cut both ways:

- **Specificity:** The maritime descriptions name concrete data types, such as bunker cost calculations, demurrage and despatch records, and port disbursement accounts, which are hard to invent convincingly at scale
- **Templated language:** The entries follow an identical structure and phrasing, which suggests automated or generated write-ups and says little about the underlying access

- **No confirmations:** No listed maritime organization had publicly confirmed an incident at the time of writing
- **Track record:** The group's earlier high-profile claims, including those against Fanatics and Transcom WorldWide, had not been publicly confirmed by the named companies at the time of writing

The October 19 deadline is the most useful test. Whether data appears, how much, and whether it matches the descriptions will show what n0n actually holds.

## What Maritime and Logistics Organizations Should Do Now

Listed or not, any organization that exchanges EDI with the companies above should plan for the possibility that its operational data appears in the October 19 release.

- **Map your shared platforms:** Identify which port community systems, EDI hubs, terminal system vendors and file transfer services carry your data, and ask them directly whether they are investigating
- **Patch and review exposed interfaces:** Check internet-facing EDI, file transfer and terminal system components for outstanding security updates and unexpected access or bulk downloads; as SOCRadar's maritime OSINT guide shows, port management and cargo tracking systems can be discoverable on search engines such as Shodan
- **Rotate integration credentials:** Reset SFTP, AS2, VAN and vendor support accounts used for EDI and terminal systems, starting with any shared or long-lived ones
- **Check infostealer exposure:** Search for employee and vendor credentials in stealer logs, since n0n's earlier access started there; the SOCRadar Dark Web Report is a free starting point
- **Close remote access gaps:** Enforce MFA on VPN and RDP, remove internet-exposed RDP, and review recent remote logins for unfamiliar sources
- **Prepare for counterparty exposure:** Draft customer and regulator communications now, because your data can leak through a partner's or vendor's breach even if your own network is clean
- **Track the group:** Follow n0n's activity and new postings on its SOCRadar group profile

## Frequently Asked Questions

### What Is the n0n Ransomware Group?

n0n is a financially motivated extortion group that emerged in September 2026. It has typically gained access with credentials stolen by infostealer malware, and it threatens to publish stolen data on its Dark Web leak site unless victims pay.

### Does n0n Deploy Ransomware?

SOCRadar's profile describes n0n as avoiding traditional ransomware and relying on data theft and extortion, although its ATT&CK mapping includes encryption and recovery-inhibition techniques.

### Which Maritime Organizations Did n0n List?

On October 12, 2026, n0n posted 38 organizations, including Santos Brasil, Ocean Network Express, Pusan Newport Company, BNCT, TTI Algeciras, Eurogate Tanger, NEOM Ports, ILCS Pelindo and Camellia Line.

### How Did n0n Access the Maritime Victims?

This has not been confirmed. Small, application-scoped data sets and the lack of infostealer credential matches for some victims point to an exposed shared application or vulnerability rather than separate intrusions.

### How Much Is n0n Demanding?

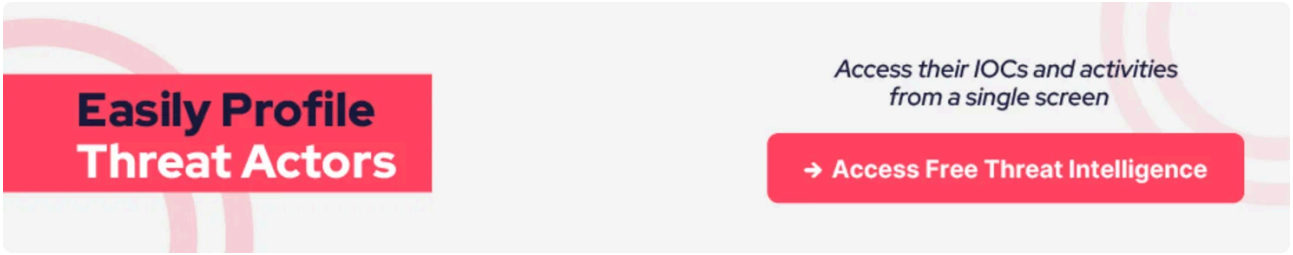
Settlement demands reviewed by SOCRadar range from USD 2.4 million to USD 14 million, payable in Bitcoin to a unique address per victim, and some pages require a 10% payment before negotiations can open.

### When Will the Maritime Data Be Published?

The maritime entries show a publication deadline of October 19, 2026, at 13:27 UTC.

### Have the Listed Companies Confirmed a Breach?

No listed maritime organization had publicly confirmed an incident at the time of writing, and the claims remain unverified.






Omer Faruk Diken

Omer is Technical Content Lead at SOCRadar, helping turn threat research into reports, blog posts, and other material for the security community. He spends most of his time working with researchers and editors to get the details right. There's usually a draft in progress and a headline he isn't quite happy with yet.

---

Source: https://socradar.io/blog/n0n-group-global-ports-shipping-leak/