ZEROFOX INTELLIGENCE

Flash

N0n Ransomware Group's Alleged Logistics Sector Breach Victims Likely Share Supplier

F-2026-10-30a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Transport and Logistics, Ransomware, Supply Chain

October 30, 2026

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 28, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | N0n Ransomware Group's Alleged Logistics Sector Breach Victims Likely Share Supplier

| Key Findings

- As of October 26, 2026, ransomware and digital extortion (R&DE) group n0n claims to have stolen data from at least 38 maritime and logistics organizations that very likely originated from one shared supplier rather than via 38 separate intrusions.
- The threat group has claimed at least 86 victims since ZeroFox first observed it on September 21, making it a fast-growing R&DE collective. N0n is very likely opportunistic rather than sector-focused, although the transport and logistics sector now comprises roughly a quarter of its current victims.
- While the claimed data is unlikely to be used to directly disrupt shipping or transport operations, it likely provides threat actors with material for cargo fraud, phishing, and intrusion planning against port terminals. However, none of the listings ZeroFox observed mention container release codes, likely limiting the most direct route to cargo theft.
- N0n is likely attempting to scale its operations. On October 26, an untested actor using the alias “nn0nn” advertised a n0n affiliate program for initial access

© 2026 ZeroFox, Inc. All rights reserved.

brokers (IABs) on a Russian-language dark web forum. As of writing, ZeroFox was unable to confirm whether the actor is associated with the group. If recruitment succeeds, victim listings will likely accelerate, and organizations that appear on them will need to determine if their exposure stems from a shared upstream source rather than a direct breach.

Details

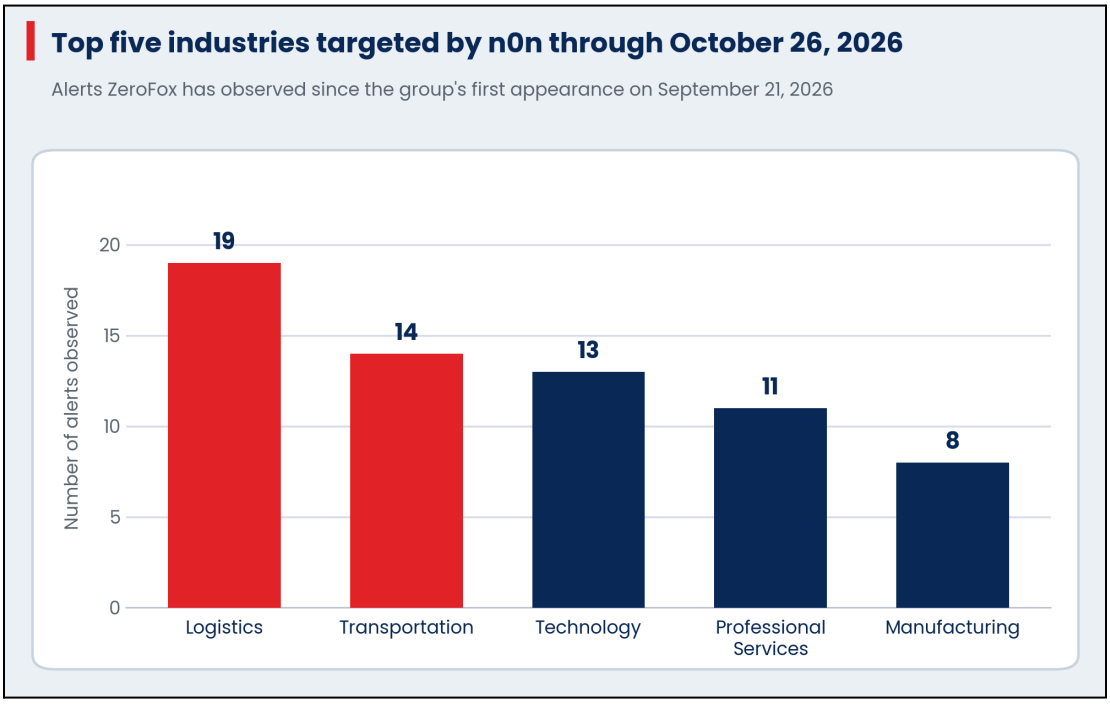
As of October 26, 2026, R&DE group n0n claims to have stolen data from at least 38 maritime and logistics organizations that very likely originated from one shared supplier rather than via 38 separate intrusions. Separately, South Korea firm Hanjin Information Systems & Telecommunication (HIST)—an IT service provider to transport, shipping, and aviation networks—confirmed a cyber incident on October 21, two days after n0n listed the firm as a victim.[1][2] HIST's confirmation of the breach likely lends credibility to some of n0n's claims.

- The n0n threat group, which first appeared in September 2026 and is very likely opportunistic rather than sector-focused, posted separate ransom demands targeting 38 organizations on October 12, with a common payment deadline of October 19.[3] The group has since updated its leak site with a download link that allegedly leads to the breached data.
- ZeroFox reviewed sample files across 20 claimed victims and noted they carry serial numbers running from roughly 36,000 to 1.1 million. Further, reviewed files for 11 victims also display dates that fall in order by serial number, which is consistent with a single system numbering support tickets for many customers. The file names appear to reference support tickets, release notes, and configuration records—material a software supplier would likely hold for its customers. ZeroFox has not independently verified the data in full and is not naming the suspected supplier.

[1] https://cloud.zerofox.com/intelligence_new/advanced_dark_web/113324
[2] hXXps://www.hist[.]co[.]kr/pr-center/news?id=1966557673
[3] https://cloud.zerofox.com/intelligence_new/advanced_dark_web/112623

© 2026 ZeroFox, Inc. All rights reserved.

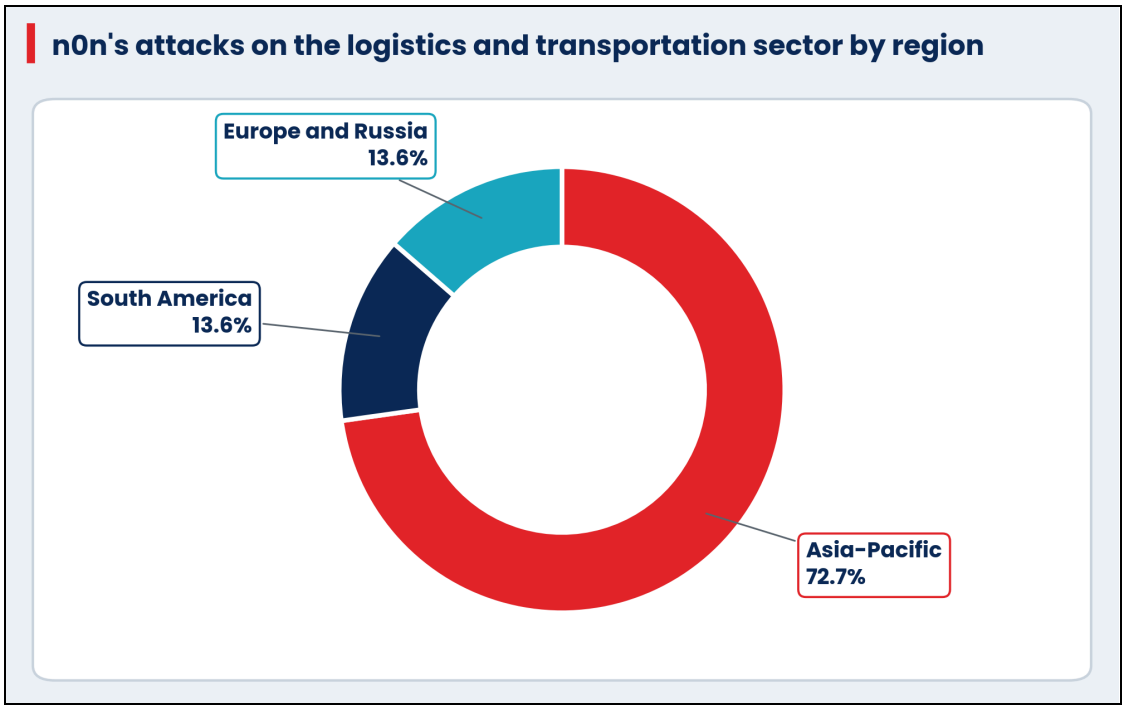
- ZeroFox noted the group has mislabeled some victims. For example, n0n tagged an inland container depot in Malaysia as South Korean, which very likely suggests unfamiliarity with the organizations and that these were not individual intrusions.



Source: ZeroFox Intelligence

- None of n0n's first 17 listings, published between September 21 and October 7, pertained to transport or logistics; instead, they included a sports retailer, a teachers' union, a pharmaceutical subsidiary, and an outsourced customer service provider.
- The Asia-Pacific concentration of n0n's transport and logistics listings likely reflects the supplier's customer base rather than regional geopolitics, and the timing of the campaign very likely reflects when n0n obtained the data.

© 2026 ZeroFox, Inc. All rights reserved.



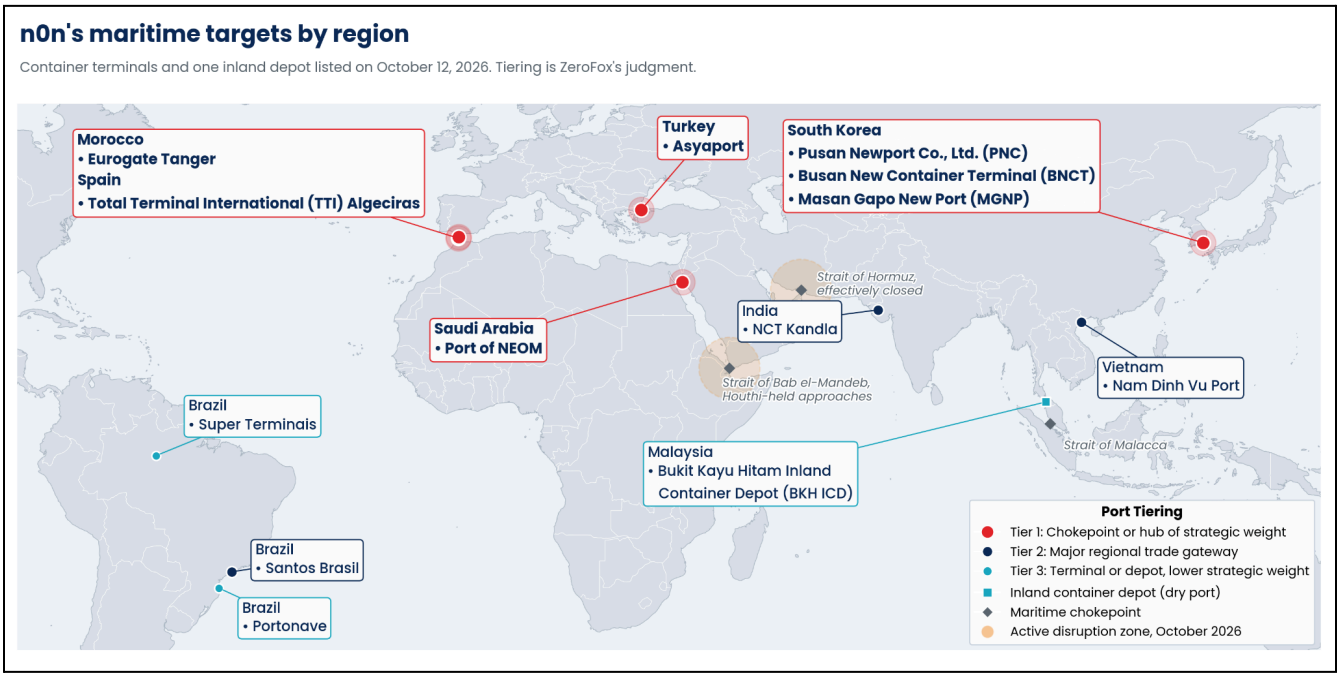
Source: ZeroFox Intelligence

While the claimed data is unlikely to be used to directly disrupt shipping or transport operations, it likely provides threat actors with material that would support cargo fraud, phishing, and intrusion planning against port terminals. The stolen records allegedly include electronic data interchange messages, booking records, gate movement logs, and stowage plans, along with system documentation and staff contact details. The victim organizations include 12 port terminals and one inland depot, which likely face the greatest downstream risk.

- Booking, gate movement, and stowage records will likely enable criminal groups to identify a container's cargo and ownership, as well as when the shipment is scheduled to be collected. System documentation, database scripts, and staff names and email addresses are likely to help attackers map terminal systems and target staff with phishing schemes and credential theft.
- Between 2011 and 2013, drug traffickers who obtained container data from systems at the Port of Antwerp-Bruges collected shipments by sending bogus drivers to

© 2026 ZeroFox, Inc. All rights reserved.

the terminal before the legitimate hauler arrived.[4] That scheme depended on container release codes; ZeroFox observed no listings within the reviewed sample files that mention container release codes, likely limiting the most direct route to cargo theft.



Source: ZeroFox Intelligence

The n0n group is likely attempting to scale its operations. On October 26, 2026, an untested actor using the alias nn0nn advertised a n0n affiliate program for IABs on RehubCom, a predominantly Russian-language dark web forum.[5] ZeroFox has not independently confirmed whether the actor is associated with the n0n R&DE group. If recruitment succeeds, victim listings will likely accelerate, and organizations that appear on them will need to determine if their exposure stems from a shared upstream source rather than a direct breach.

[4] hXXps://www.theregister[.]com/offbeat/2013/06/18/drug-gang-hacks-into-belgian-seaport-cops-seize-tonne-of-smack/729944
[5] https://cloud.zerofox.com/intelligence_new/advanced_dark_web/113472

© 2026 ZeroFox, Inc. All rights reserved.

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.

© 2026 ZeroFox, Inc. All rights reserved.

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%

© 2026 ZeroFox, Inc. All rights reserved.